

editorial reverté s. a.

Lecciones de álgebra moderna

P. DUBREIL

M. L. DUBREIL-JACOTIN

Segunda edición

P. DUBREIL

M. L. DUBREIL-JACOTIN

Profesores de la Facultad de Ciencias de París

LECCIONES DE ALGEBRA MODERNA

Segunda edición



Editorial Reverté, S. A.
Barcelona - Buenos Aires - México

Título de la obra original:

Leçons d'Algèbre Moderne

Editada por Dunod, París

Versión española de la edición
francesa revisada y corregida
por los autores, a cargo del

Dr. R. RODRIGUEZ VIDAL

Catedrático de la Facultad
de Ciencias de Zaragoza

Propiedad de EDITORIAL REVERTÉ, S. A. Encarnación. 86 Barcelona (12)

Reservados todos los derechos. Ninguna parte del material cubierto por este título de propiedad literaria puede ser reproducida, almacenada en un sistema de informática o transmitida de cualquier forma o por cualquier medio electrónico, mecánico, fotocopia, grabación u otros métodos sin el previo y expreso permiso por escrito del editor.

Edición en español

© **EDITORIAL REVERTÉ, S. A., 1971 1975**

Impreso en España Printed in Spain

ISBN - 84 - 291 - 5070 - 6

Depósito legal B. 37534 1975
Litoclub - Nápoles, 300 - Barcelona

PRÓLOGO

Si el estudio del Álgebra atrae cada vez más a los estudiantes, es, ciertamente, porque ya no se pueden hacer Matemáticas sin Álgebra; y también es, sin duda, porque esta disciplina tiene su propio interés y su atractivo particular. En el curso del desarrollo prodigioso que ha tenido en los últimos cuarenta años, el Álgebra se ha desembarazado de técnicas enrevesadas, para convertirse en una ciencia seductora por la elegancia de sus métodos y demostraciones. Se ve en toda su pureza al razonamiento matemático operar sobre una multitud de nociones, de las que no se sabe bien si es mejor decir, que cada una es perfectamente simple y natural, o que el conjunto, es un extraordinario producto de la imaginación humana.

El poder formativo del Álgebra es considerable. Así, se ha creado en nuestras Facultades una "opción algebraica" en la licenciatura para la enseñanza, y es el programa (máximo) de esa opción el objeto de este tratado. Éste no pretende ser más que un libro dedicado a los estudiantes; ésta es la razón, por ejemplo, de que no contenga indicaciones bibliográficas.

El libro es autónomo, vuelve a tomar desde el principio, con un espíritu diferente, las nociones fundamentales de Álgebra de los estudios preparatorios. Se ha insistido en destacar algunas ideas directrices. Tomadas de la teoría de conjuntos, las nociones de familia de Moore y de clausura de Moore dominan lo concerniente a la generación de estructuras algebraicas. Las nociones de retículo y de grupos con operadores, permiten la aproximación entre la teoría de grupos, la de anillos y la de espacios vectoriales. El axioma de Zorn, estudiado en sí mismo de modo completo, conduce a la existencia de un ideal maximal incluyendo a un ideal dado, a la de base en un espacio vectorial de dimensión infinita y a la de un suplementario para cualquier subespacio, así como a la existencia de clausura algebraica de un cuerpo conmutativo.

No es necesario decir que debemos mucho a los tratados de Álgebra escritos antes que éste por numerosos autores. Expresamos nuestra gratitud a J. ARBAULT y a P. LEFEBVRE que nos han ayudado en la corrección de pruebas con una multitud de valiosas sugerencias.

Agradecemos calurosamente a la Editorial DUNOD que su iniciativa contribuya tan afortunadamente al desarrollo de la edición matemática.

PAUL DUBREIL, MARIE-LOUISE DUBREIL-JACOTIN

Nota del traductor

Unas pocas palabras de explicación y de gratitud.

Creemos hacer un trabajo útil para todos los estudiantes de habla hispana al ofrecerles la versión de un texto cuyo valor didáctico se ha acreditado con una rapidez inusitada, aunque no sorprendente para quienes conocían el valor de los autores. El traductor ha tenido algunas veces la tentación de modificar la nomenclatura, para ponerla más de acuerdo con la clásica en castellano, o algunos detalles de exposición, para buscar la más perfecta adaptación a nuestros programas. Pero ha resistido esas tentaciones (bien disculpables para todo profesor de Álgebra) y ha decidido ofrecer una traducción disciplinada y fiel. Debe hacer constar la valiosa ayuda de los profesores adjuntos señores RAMIRO y ONIEVA.

Los autores han acrecentado los motivos para la gratitud del traductor al comunicarle, para que fuesen recogidas por primera vez en esta edición española, las correcciones, que el uso de su propio libro les ha sugerido. Numerosos detalles de la primera edición francesa (1961) han sido, pues, mejorados en ésta, por la amable deferencia de sus autores.

El público lector de temas matemáticos es siempre minoritario, y ello hace altamente meritorio el gesto de los pocos editores que por vocación cultural, más que comercial, se dedica a él. Gracias, pues, a EDITORIAL REVERTÉ, por el interés y cuidado que ha puesto en la aparición de esta edición.

R. R. V.
(1963)

Nota a la segunda edición

Al publicar esta segunda edición (revisada) del texto de Dubreil y Dubreil-Jacotin, resulta oportuno advertir que la Editorial Reverté ha publicado recientemente una traducción del libro de A. Bigard, M. Crestey y J. Grappy, *Problemas de Álgebra Moderna*, el cual constituye una ilustración práctica de estas lecciones teóricas, cuyo espíritu y estilo conservan. Sin embargo, ambos libros son autónomos en su empleo.

R. R. V.
(1971)

Índice de materias

CAPÍTULO I

I. LEYES DE COMPOSICIÓN

§ 1.	Observaciones generales sobre algunas operaciones clásicas	1
§ 2.	Leyes de composición	2
§ 3.	Conjuntos con una ley de composición interna	4
§ 4.	Construcción de conjuntos con una ley de composición interna	6
§ 5.	Relaciones de equivalencia compatibles con una ley de composición interna ...	12
§ 6.	Aplicaciones notables de un conjunto con una ley de composición interna en o sobre otro: homomorfismos; isomorfismos	18
§ 7.	Elementos notables de un conjunto con una ley de composición interna	25
§ 8.	Partes notables de un conjunto E con una ley de composición interna	32

CAPÍTULO II

II. SEMIGRUPOS. GRUPOS

§ 1.	Asociatividad. Semigrupos	38
§ 2.	Grupos. Axiomática de grupo	46
§ 3.	Ejemplos de grupos	51
§ 4.	Grupos asociados a otro dado o a varios subgrupos. Subgrupos de un grupo ...	53
§ 5.	Homomorfismo en teoría de grupo; subgrupos distinguidos; descomposición en clases: automorfismos internos	57
§ 6.	Leyes de composición externa. Espacios homogéneos. Teoremas de Sylow ...	67
§ 7.	Leyes de composición externa. Grupos operadores.	80

CAPÍTULO III

III. GENERACIÓN DE GRUPOS

§ 1.	Sistemas de generadores: conmutadores. Unión completa	84
§ 2.	Grupo simétrico	87
§ 3.	Grupos monógenos; Grupos cíclicos	93
§ 4.	Grupos de tipo finito	98
§ 5.	Inmersión de un semigrupo abeliano con ley de simplificación en un grupo ...	100
§ 6.	Grupos libres	103
§ 7.	Grupos abelianos libres	109

CAPÍTULO IV

IV. ANILLOS Y CUERPOS

§ 1.	Leyes de composición distributivas	111
§ 2.	Anillos. Subanillos. Grupos de las unidades	116
§ 3.	Cuerpos	124
§ 4.	Grupo aditivo de un anillo. Característica	129
§ 5.	Anillos de series formales y anillos de polinomios sobre un anillo conmutativo ...	133
§ 6.	Propiedades aritméticas en los dominios de integridad con elemento unidad. Anillos factoriales. Anillos euclídeos	148
§ 7.	Ideales de un anillo	162
§ 8.	Ideales maximales. Ideales primos	176

CAPÍTULO V

V. CONJUNTOS ORDENADOS. RETÍCULOS

§ 1.	Conjuntos ordenados. Cadenas	183
§ 2.	Elementos notables eventuales en un conjunto ordenado E	185
§ 3.	Semirretículos	187
§ 4.	Retículos	188
§ 5.	Definición algebraica de un semirretículo o de un retículo	198
§ 6.	Retículos distributivos; retículos complementados	203
§ 7.	Retículos de Boole	209
§ 8.	Retículos modulares	218
§ 9.	Conjuntos con una relación de orden y una ley de composición interna	229
§ 10.	Estudio del retículo multiplicativo de los ideales de un anillo conmutativo	234
§ 11.	Residuación. Aplicación al estudio de las intersecciones de ideales primarios ...	240

CAPÍTULO VI

VI. AXIOMA DE ZORN

§ 1.	Conjuntos inductivos; enunciado del axioma de Zorn	249
§ 2.	Aplicaciones del teorema de Zorn	252
§ 3.	Axiomas equivalentes al de Zorn	256

CAPÍTULO VII

VII. ANILLOS NOETHERIANOS

§ 1.	Retículos con condiciones de cadena	262
§ 2.	Anillos noetherianos	265
§ 3.	Anillos principales	268
§ 4.	Propiedades de los ideales en un anillo noetheriano A	270
§ 5.	Descomposición noetheriana	272

CAPÍTULO VIII

VIII. COMPLEMENTOS DE LA TEORÍA DE LOS GRUPOS

§ 1.	Grupos con operadores	275
------	-----------------------------	-----

§ 2.	Segundo teorema del isomorfismo	284
§ 3.	Series normales. Series de composición. Teorema de Jordon-Hölder	288
§ 4.	Producto directo de grupos	291
§ 5.	Rango de un grupo abeliano G	303
§ 6.	Grupos abelianos de tipo finito	308

CAPÍTULO IX

IX. ESPACIOS VECTORIALES

§ 1.	Espacios vectoriales como grupos con operadores	316
§ 2.	Aplicaciones lineales y matrices	325
§ 3.	Dimensión del espacio imagen. Aplicaciones lineales y matrices regulares o singulares	339
§ 4.	Cambio de base	347
§ 5.	Ecuación mínima	350
§ 6.	Ecuación característica	359

CAPÍTULO X

X. CUERPOS. ECUACIONES ALGEBRAICAS

§ 1.	Extensiones simples	368
§ 2.	Cuerpo de ruptura. Cuerpo de descomposición	371
§ 3.	Extensiones finitas elementos algebraicos	379
§ 4.	Ecuaciones algebraicas	383
§ 5.	Enteros algebraicos	393
§ 6.	Raíces de la unidad	398
§ 7.	Campos de Galois	399
§ 8.	Teorema del elemento primitivo	404
§ 9.	Teorema de Wedderburn	406
§ 10.	Clausura algebraica de un cuerpo k	409
§ 11.	Teorema de los ceros de Hilbert	412
§ 12.	Teoría de Galois	415
§ 13.	Algunos complementos sobre las propiedades del grupo de Galois de un polinomio separable $f(x) \in K[x]$	424

INDICE ALFABÉTICO.....	425
------------------------	-----

CAPÍTULO PRIMERO

LEYES DE COMPOSICIÓN

§ 1. Observaciones generales sobre algunas operaciones clásicas

En el curso del estudio de las Matemáticas elementales hemos realizado la suma y la multiplicación de números naturales $1, 2, \dots$, y de números racionales (representados por fracciones); más tarde la suma y multiplicación de números racionales de cualquier signo; por fin, la suma y multiplicación de números reales y de números complejos.

La resolución de las ecuaciones:

$$b + x = a, \quad by = a,$$

donde a y b son dos números dados, nos llevó a las operaciones inversas, sustracción y división.

Pero aquí la existencia de la diferencia $x = a - b$ y la del cociente exacto $y = b : a$ depende esencialmente del *conjunto de números considerado*: en el conjunto $\mathbf{Q}$ de los números racionales (≥ 0), en el conjunto $\mathbf{R}$ de números reales (≥ 0), en el conjunto $\mathbf{C}$ de los números complejos, la sustracción es siempre posible, mientras que no sucede lo mismo en el conjunto $\mathbf{N}$ de los números naturales, ni en el conjunto $\mathbf{Q}^+$ de los números racionales positivos. En $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, el cociente exacto de a por b existe mediante la sola condición $b \neq 0$; no sucede lo mismo en $\mathbf{N}$, ni en el conjunto $\mathbf{Z}$ de los enteros relativos (es decir ≥ 0).

En otro orden de ideas, consideremos los movimientos, en geometría, y su composición, que a dos movimientos dados α, β , asocia el movimiento $\beta \circ \alpha$ que se obtiene realizando primero α y después β . Si α y β son dos traslaciones, tenemos

$$\alpha \circ \beta = \beta \circ \alpha$$

pero esta igualdad no es cierta para dos movimientos α, β cualesquiera: esto

se ve, por ejemplo, en geometría plana, cuando α y β son las simetrías con relación a dos puntos distintos O y O' (fig. 1); tenemos, con la notación de la figura

$$(\beta \circ \alpha) O = \beta O = O_1$$

$$(\alpha \circ \beta) O = \alpha O_1 = O_2.$$

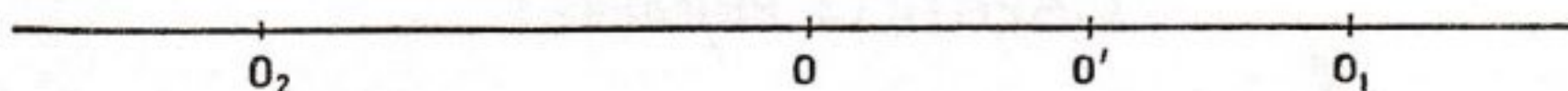


FIG. 1.

He aquí, pues, que una propiedad de la operación $\circ$ depende también del conjunto sobre el que esta operación actúa.

Es indispensable pues, si se quiere estudiar correctamente una operación, *no separar ésta del conjunto de los elementos sobre los cuales se realiza*; El lenguaje de la teoría de conjuntos nos va a permitir introducir de una manera precisa y general, la noción de *ley de composición*, fundamental en álgebra moderna.

§ 2. Leyes de composición

Expresamos con la notación clásica $a \in E$ (" a pertenece a E ") que un ente a es elemento de un conjunto E . Dado el conjunto E , consideramos como definido el conjunto de pares ordenados (a, b) donde $a \in E$, $b \in E$; la locución *pares ordenados* significa, que se distinguen en cada par (a, b) el *primer* elemento a y el *segundo* elemento b . El conjunto de estos pares es por definición el *conjunto producto cartesiano* de E por sí mismo, designado por $E \times E$.¹

Se llama *ley de composición interna* definida sobre E , toda ley T que asocie a cada par ordenado (a, b) de elementos de E un elemento c de E , imagen de este par; tal ley de composición no es más que una aplicación τ del conjunto producto $E \times E$ en E .

$$(\tau) \quad (a, b) \rightarrow c.$$

Se dice también que T define en E una *operación binaria*; a es el *primer término*, b el *segundo término*, c el *resultado*; es cómodo escribir

$$a T b = c$$

(que al leer se enuncia " a truc b igual a c ").

¹ Dados los conjuntos A y B , si a cada $a \in A$ corresponde un $b \in B$, y sólo uno, se tiene definida una *aplicación* (o *función uniforme*) α de A en B , que se indica poniendo $\alpha: A \rightarrow B$. El ele-

Puede suceder que deban considerarse simultáneamente varias leyes de composición interna en un mismo conjunto; se emplean entonces otros símbolos tales como $\perp$ ("antitruc"), $*$ ("estrella"), o bien letras $O, O_1 \dots$. Por otra parte, conocemos bien los símbolos propios de las operaciones usuales: $+$ (*notación aditiva*: adición de números, de funciones...); $\cdot$ o nada (*notación multiplicativa*: multiplicación de números, de funciones...); $\cap$ (intersección de partes de un conjunto), $\cup$ (unión de partes de un conjunto), $\wedge$ (producto vectorial), etc. ... El símbolo de una cierta operación algebraica es a menudo utilizado para una ley de composición abstracta que tiene propiedades análogas. Se debe observar que, para la composición de las aplicaciones, el signo $\circ$ es utilizado *con transposición* de los términos, así que $\beta \circ \alpha$ indica la aplicación obtenida efectuando primero α , después β , de modo que

$$(\alpha, \beta) \rightarrow \gamma$$

se escribe

$$\gamma = \beta \circ \alpha.$$

Observaciones. — 1. Supondremos generalmente que el resultado $c = a \mathsf{T} b$ existe cualquiera que sea la elección de a y de b en el conjunto E^1 ; se expresa esto diciendo que T es una ley de composición interna *definida totalmente*. Desde este punto de vista, la sustracción en el conjunto $\mathbf{N}$ de números naturales, no puede ser considerada como una tal ley de composición.

2. También supondremos que, si los términos a, b son fijos, el resultado $c = a \mathsf{T} b$ es *único*, lo cual se expresa diciendo que T es una ley de composición *uniforme*.

3. Podemos evidentemente eximirnos de las restricciones precedentes, y considerar leyes de composición definidas solamente sobre ciertas partes de $E \times E$, o para las que el resultado sea, no un elemento, sino una parte de E (leyes *multiformes*). La generalización siguiente nos será más útil.

Consideremos tres conjuntos cualesquiera A, B, C , distintos o no, y el conjunto producto $A \times B$ de los primeros, esto es, el conjunto de pares (a, b) donde $a \in A, b \in B$.

Llamaremos de forma general *ley de composición* a toda aplicación $(a, b) \rightarrow c$ ($a \in A, b \in B, c \in C$) del conjunto $A \times B$ en el conjunto C .

El elemento b se llama *imagen* (o *representación*) del a ; mientras que a es *original* (o *imagen recíproca*) del b . Si todo elemento de B es imagen de al menos uno de A , la aplicación se llama *exhaustiva* (o de A sobre B , en francés "*surjective*"). Si cada elemento de B tiene a lo más un original en A , la aplicación es *inyectiva* (o *función univalente*). Una aplicación inyectiva y exhaustiva se llama *biyectiva* (o *biunívoca*). (N. del T.)

¹ También cuando b coincida con a , es decir, para cada elemento consigo mismo. (N. del T.)

Ejemplos. — 1. Consideremos tres conjuntos E_1, E_2, E_3 , y llamemos:

A el conjunto de aplicaciones de E_1 en E_2

B el conjunto de aplicaciones de E_2 en E_3

C el conjunto de aplicaciones de E_1 en E_3 .

Al par (α, β) formado por una aplicación $\alpha \in A : x_1 \rightarrow \alpha x_1 = x_2$ y por una aplicación $\beta \in B : y_2 \rightarrow \beta y_2 = y_3 \in E_3$, asociemos la *aplicación compuesta* $\gamma = \beta \circ \alpha \in C$ definida por $\gamma x_1 = \beta(\alpha x_1)$. (Se escribe más brevemente $\gamma = \beta\alpha$, supuesto que no haya temor a confusiones). Tenemos aquí una ley de composición

$$(\alpha, \beta) \rightarrow \gamma$$

en la cual los dos términos α, β y el resultado γ pertenecen a conjuntos A, B, C , en general diferentes.

2. Sean p y q dos enteros naturales, distintos o no; designemos respectivamente por A, B los conjuntos de polinomios ¹ en x , con coeficientes reales de grados p, q . La multiplicación de un polinomio $f \in A$ por un polinomio $g \in B$ da un polinomio fg perteneciente al conjunto C de los polinomios de grado $p + q$: constituye una ley de composición, que es una aplicación del conjunto $A \times B$ en el conjunto C .

3. La formación del producto escalar $\vec{V}_1 \cdot \vec{V}_2 = p$ de dos vectores libres $\vec{V}_1, \vec{V}_2$ del espacio euclídeo real de tres dimensiones, es una ley de composición en la cual los conjuntos A, B , coinciden con el conjunto E de esos vectores libres, mientras C es el conjunto $\mathbf{R}$ de los números reales.

Cuando los tres conjuntos A, B, C , que intervienen en la definición de una ley de composición coinciden con un mismo conjunto E , se tiene una ley de *composición interna* definida en E .

Si A y C coinciden con un mismo conjunto E , y B es diferente de E , se tiene una *ley de composición externa a la derecha*; los elementos de B se llaman entonces *multiplicadores* u *operadores a la derecha*.

Si B y C coinciden con un mismo conjunto E , y A es diferente de E , se tiene una *ley de composición externa a la izquierda*; los elementos de A son, para los de E , *operadores* o *multiplicadores a la izquierda*. Por ejemplo, definiendo como se sabe el producto $a\vec{V}$ de un vector libre (real) $\vec{V}$ por el número real a , se introduce una ley de composición externa a la izquierda; A es el conjunto $\mathbf{R}$ de los números reales, mientras que B y C coinciden con el conjunto E de los vectores libres (reales).

§ 3. Conjuntos con una ley de composición interna

Consideremos un conjunto E con una ley de composición interna denotada por T . Cuando empleemos la notación multiplicativa o la notación aditiva, il-

¹ Volveremos más tarde (cap. IV, § 5) sobre la noción de polinomio; esta noción es utilizada aquí en su sentido elemental.

maremos a E un conjunto multiplicativo o un conjunto aditivo, respectivamente.

Cuando E es un *conjunto finito*¹, $E = \{a_1, a_2, \dots, a_n\}$ se le puede representar, o incluso definir, por su *tabla*, es decir por una tabla de doble entrada en la cual figura en la intersección de la fila de orden i con la columna de orden j , el elemento $a_i \top a_j$.

Ejemplos. — 1. Consideremos el conjunto $\{a_1, a_2, a_3\}$ con la ley de composición definida por $x \top y = y$. En tal caso tendremos la tabla

	a_1	a_2	a_3
a_1	a_1	a_2	a_3
a_2	a_1	a_2	a_3
a_3	a_1	a_2	a_3

2. En el conjunto $E = \{a, b, c, d\}$, la tabla

	a	b	c	d
a	a	a	a	a
b	b	a	a	a
c	c	b	a	a
d	d	c	b	a

define una cierta ley de composición interna.

3. Varias leyes de composición fundamentales se derivan de la adición de números naturales. Para definir a ésta, partiremos de un sistema de axiomas que caracteriza el conjunto $\mathbf{N} = \{1, 2, \dots, n, \dots\}$ de dichos números. El sistema

¹ Recordemos que un conjunto es *finito* y contiene n elementos (n , número natural) si existe una *bijección* de E sobre el conjunto $\{1, 2, \dots, n\}$ (o, si se quiere, una *correspondencia biunívoca* entre E y este conjunto). No es necesario hacer intervenir los números naturales (cuyo conjunto es infinito) para definir los conjuntos finitos: un conjunto finito es un conjunto F con una ley de ordenación total $a \leq b$ tal, que toda parte no vacía de F tenga un primer elemento, que todo elemento de F distinto del primero tenga un precedente, y que F posea un elemento último.

de PEANO es el siguiente:

1. $\mathbf{N}$ contiene al menos un elemento a tal que existe una biyección β de $\mathbf{N}$ sobre $\mathbf{N} - \{a\}$.

2. Sea $A \subseteq \mathbf{N}$. Si

1.º $a \in A$,

2.º A es estable con relación a β (es decir $\beta(A) \subseteq A$, lo que aquí puede escribirse $\beta(A) \subseteq A - \{a\}$), entonces, tenemos la igualdad

$$A = \mathbf{N} \quad (\text{principio de } recurrence)^1$$

Llamamos 1 al elemento a , 2 al elemento $\beta(a)$, 3 al elemento $\beta(2)$, etc.

Se define por recurrencia la *suma*, $n + p$, poniendo

$$\begin{aligned} n + 1 &= \beta(n) \\ n + \beta(p) &= \beta(n + p) \end{aligned}$$

Y también se puede definir la multiplicación, poniendo

$$n \cdot 1 = n \quad n \cdot \beta(p) = np + n.$$

§ 4. Construcción de conjuntos con una ley de composición interna

Expondremos ahora algunos procedimientos importantes que permiten, dados ciertos conjuntos con leyes de composición interna, construir un nuevo conjunto con ley de composición interna.

1.º Sea $\mathcal{F}$ el conjunto de las funciones f , o un conjunto de funciones, definidas sobre un conjunto dado X , y tomando sus valores en un conjunto dado E con una ley de composición T :

$$f \quad x \rightarrow y = f(x) \quad (x \in X, \quad y \in E).$$

Si f y g son dos funciones de $\mathcal{F}$, asociemos a todo elemento x de X el elemento $f(x) \mathsf{T} g(x)$ de E ; obtendremos así una función

$$x \rightarrow f(x) \mathsf{T} g(x)$$

que es, *por definición*, la función $f \mathsf{T} g$: tenemos así en $\mathcal{F}$, una ley de composición interna, definida a partir de la de E ; se representa, para abreviar, esta nueva ley una composición, que opera en $\mathcal{F}$ por el mismo signo T que la antigua que opera en E .

¹ Sinónimo de "principio de inducción", que es la usual expresión española. (N. del T.)

2.º Sean los conjuntos E_1, E_2 , y designemos aquí para mayor claridad, sus operaciones respectivas por T_1, T_2 . Consideremos el conjunto producto $P = E_1 \times E_2$. Poniendo para dos pares $(a_1, a_2), (b_1, b_2)$.

$$(a_1, a_2) T (b_1, b_2) = (a_1 T_1 b_1, a_2 T_2 b_2)$$

definimos en P una ley de composición T . Sucede a menudo que las leyes de composición T_1, T_2, T se indican por medio de un mismo símbolo.

Este procedimiento se extiende inmediatamente a cualquier número finito k de conjuntos $E_1, \dots, E_k$. Se observará que interviene en la definición del producto de dos fracciones (multiplicación de numeradores y denominadores entre sí), y en la adición de vectores (la componente de orden i del vector suma, es la suma de las componentes homólogas).

3.º Sea A una parte de un conjunto E con la ley de composición interna $T, A \subseteq E$. Si para todo par de elementos a_1, a_2 de A , el resultado $a_1 T a_2$ de la operación pertenece a A , se dice que A es una *parte estable* para la operación T de E .

Se puede, pues considerar la parte A como un conjunto en el que se define una ley de composición, que es la dada en E , aplicada a los elementos de A .

Esta ley de composición, que opera sólo sobre los elementos de A , se llama *restricción en A o traza sobre A* , de la ley de composición de E . Se la denota generalmente con el mismo símbolo que la ley de composición en E .

4.º Consideremos el conjunto de las partes $\mathcal{P}(E)$ de E ; sea T la ley de composición de E .

Si A y B son dos partes *no vacías* de E , convengamos en designar por $A T B$ el conjunto de resultados $a T b$ cuando a y b recorren respectivamente A y B ;

$$A T B = \{ a T b ; a \in A, b \in B \}.$$

Designamos ahora por $\emptyset$ la parte vacía, y pongamos

$$X T \emptyset = \emptyset T X = \emptyset$$

para cualquier parte $X \in \mathcal{P}(E)$. Así hemos definido, a partir de la ley de composición T dada en E , una ley de composición interna en $\mathcal{P}(E)$ que, según el uso, designaremos con el mismo símbolo.

Se cumplen las siguientes importantes reglas de cálculo ¹

¹ Estas reglas hacen intervenir, con la ley de composición que ha sido definida, la *relación de inclusión* de partes ($A \subseteq A'$ si todo elemento de A es elemento de A'), la *unión* de partes: (Si $\mathcal{F}$ es una familia de partes de E , es decir un subconjunto de $\mathcal{P}(E)$, la unión $\mathcal{R} = \bigcup_{X \in \mathcal{F}} X$ es el conjunto de elementos de E que pertenecen al menos a una parte $X \in \mathcal{F}$), y la *intersección* de

R_1 $A \subseteq A'$ implica $A \top B \subseteq A' \top B$
evidente según las definiciones;

$$R_2 \quad A \top \left(\bigcup_{X \in \mathcal{F}} X \right) = \bigcup_{X \in \mathcal{F}} (A \top X), \quad \left(\bigcup_{X \in \mathcal{F}} X \right) \top B = \bigcup_{X \in \mathcal{F}} (X \top B);$$

Para establecer cada una de estas dos igualdades, basta observar que un elemento cualquiera del primer miembro pertenece al segundo, e inversamente;

$$R_3 \quad A \top \left(\bigcap_{X \in \mathcal{F}} X \right) \subseteq \bigcap_{X \in \mathcal{F}} (A \top X), \quad \left(\bigcap_{X \in \mathcal{F}} X \right) \top B \subseteq \bigcap_{X \in \mathcal{F}} (X \top B);$$

todo elemento del primer miembro pertenece, en efecto, al segundo, a causa de R_1 ; pero aquí, la igualdad no es cierta en general. Consideremos por ejemplo el conjunto $\{a, b, c, d\}$ de la pág. 5 y tomemos

$$A = \{b\}, \quad X_1 = \{a, b\}, \quad X_2 = \{a, c\}$$

Tenemos

$$\begin{aligned} X_1 \cap X_2 &= \{a\} & A \top (X_1 \cap X_2) &= \{b\} \\ A \top X_2 &= A \top X_1 = \{a, b\} & (A \top X_2) \cap (A \top X_1) &= \{a, b\}. \end{aligned}$$

Observación. — Cuando se trata de una parte $\{x\}$ formada por un solo elemento x , se escribe ordinariamente $x \top A$ en vez de $\{x\} \top A$, y $A \top x$ en vez de $A \top \{x\}$.

5.º Se dice que una familia $\mathcal{F}$ de partes de E es una *familia de Moore* si E pertenece a ella y, además, con cualesquiera partes de E que estén en la familia, está también su intersección. Estas dos propiedades de $\mathcal{F}$ se formulan así:

$$\begin{aligned} M_1 & \quad E \in \mathcal{F} \\ M_2 & \quad \text{si } \mathcal{F}' \subseteq \mathcal{F}, \text{ se tiene } \bigcap_{F \in \mathcal{F}'} F \in \mathcal{F}. \end{aligned}$$

De esta definición resulta que *la intersección de familias de Moore relativas al mismo conjunto E no es nunca vacía y es ella misma una familia de Moore.*

Por ejemplo, si se consideran las partes de un conjunto E estables para una aplicación de E en E , constituyen evidentemente una familia de Moore; y las partes de E estables para una familia de aplicaciones constituyen asimismo una familia de Moore.

partes (la intersección $I = \bigcap_{X \in \mathcal{F}} X$ es el conjunto de los elementos de E que pertenecen simultáneamente a toda parte $X \in \mathcal{F}$).

Teorema 1. — *Para toda parte A de E , existe una parte mínima $\bar{A} \in \mathcal{F}$ que contiene a A .*

Según M_1 , el conjunto $\mathcal{F}'$ de los elementos F de $\mathcal{F}$ que contienen a A no es vacío; según M_2 , $\bar{A} = \bigcap_{F \in \mathcal{F}'} F$ pertenece a $\mathcal{F}$; ahora bien, tenemos $A \subseteq \bar{A}$; es pues el menor elemento de $\mathcal{F}$ que contiene a A .

Observación. — *Si $A \in \mathcal{F}$, se tiene $A = \bar{A}$, e inversamente.*

Se llama aplicación de *clausura* de Moore (μ) asociada a $\mathcal{F}$ la aplicación de $\mathcal{P}(E)$ sobre $\mathcal{F}$ que a toda parte A de E asocia $\bar{A}$.¹

Dicho esto supongamos que E tenga la ley de composición τ , y designemos igualmente por τ la ley de composición del conjunto de las partes $\mathcal{P}(E)$, (ver 4.º). Siendo $\mathcal{F}$ una familia de partes de E , las relaciones $A_1 \in \mathcal{F}$, $A_2 \in \mathcal{F}$ no implican en general $A_1 \tau A_2 \in \mathcal{F}$. Pero cuando $\mathcal{F}$ es una familia de Moore, se puede definir una ley de composición $\bar{\tau}$, a partir de τ , poniendo:

$$F_1 \bar{\tau} F_2 = \overline{F_1 \tau F_2} \quad (F_1, F_2 \in \mathcal{F})$$

donde $\overline{F_1 \tau F_2}$ designa el *mínimo elemento de $\mathcal{F}$ que contiene a $F_1 \tau F_2$* .

Este procedimiento es fundamental y veremos numerosas e importantes aplicaciones del mismo. Demos ahora solamente un ejemplo bien sencillo.

Ejemplo. — Sea $\mathcal{F}$ el conjunto de partes de E que contienen un elemento dado a . Tenemos

$$\bar{A} = A \cup \{a\},$$

y

$$F_1 \bar{\tau} F_2 = (F_1 \tau F_2) \cup \{a\}.$$

En este ejemplo, como en la definición general, se ve que la aplicación $\bar{\tau}$ de $\mathcal{F} \times \mathcal{F}$ en $\mathcal{F}$ correspondiente a la ley de composición $\bar{\tau}$ es el resultado de la composición de la aplicación τ de $\mathcal{P}(E) \times \mathcal{P}(E)$ en $\mathcal{P}(E)$, restringida a $\mathcal{F} \times \mathcal{F}$, y de la aplicación de clausura $A \rightarrow \bar{A}$ de $\mathcal{P}(E)$ en $\mathcal{F}$, restringida a $\tau(\mathcal{F} \times \mathcal{F})$.

Estudiemos más a fondo la aplicación

$$(\mu) \quad A \rightarrow \bar{A}$$

de $\mathcal{P}(E)$ en $\mathcal{F}$; esta aplicación, asociada a la familia de Moore $\mathcal{F}$, tiene las tres propiedades siguientes:

¹ La parte $\bar{A}$, clausura de A , se llama en otros autores *adherencia* de A , y se indica con la misma notación. (N. del T.)

α) es *extensiva*, es decir

$$A \subseteq \bar{A}$$

β) es *isótoma*, es decir

$$A \subseteq B \text{ implica } \bar{A} \subseteq \bar{B}$$

γ) es *idempotente*, es decir

$$\bar{\bar{A}} = \bar{A}$$

(pues $\bar{A} \in \mathcal{F}$).

Es notable el hecho de que inversamente, toda aplicación

$$(\varphi) \quad A \rightarrow \bar{A}$$

de $\mathcal{P}(E)$ en $\mathcal{P}(E)$ que verifique las tres propiedades precedentes, α , β , γ permite definir en $\mathcal{P}(E)$ una familia de Moore $\mathcal{F}$; además φ es la clausura asociada a $\mathcal{F}$.

Llamemos en efecto *partes cerradas* a las imágenes $F = \bar{X} (= \varphi(X))$ y designemos por $\mathcal{F}$ el conjunto de esos elementos;

$$\mathcal{F} = \varphi(\mathcal{P}(E)) = \{ \varphi(X), X \in \mathcal{P}(E) \}.$$

Según α tenemos $E = \bar{E}$, luego $E \in \mathcal{F}$. Sea ahora $\mathcal{F}'$ una subfamilia de $\mathcal{F}$

y $I = \bigcap_{F \in \mathcal{F}'} F$. Tenemos $I \subseteq \bar{I}$. Pero, por otra parte la isotomía β da

$$\bar{I} = \overline{\bigcap_{F \in \mathcal{F}'} F} \subseteq \bar{F} \quad \text{cualquiera que sea } F \in \mathcal{F}';$$

luego

$$(1) \quad \bar{I} \subseteq \bigcap_{F \in \mathcal{F}'} \bar{F}.$$

Ahora bien, según la idempotencia γ , para todo $F = \bar{X} \in \mathcal{F}$, tenemos

$$\bar{F} = \bar{\bar{X}} = \bar{X} = F;$$

y, por lo tanto, (1) se escribe

$$\bar{I} \subseteq \bigcap_{F \in \mathcal{F}'} F = I$$

de donde $I = \bar{I}$, luego $I \in \mathcal{F}$, y por ende $\mathcal{F}$ es una familia de Moore.

Si $F (\in \mathcal{F})$ contiene a A , tenemos $\bar{A} \subseteq \bar{F} = F$; $\bar{A}$ es pues el menor elemento de $\mathcal{F}$ que contiene a A : es decir, que φ es la aplicación asociada a la familia de Moore $\mathcal{F}$.

Desde este punto de vista, es claro que si F_1, F_2 son dos partes cerradas no hay razón alguna para que $F_1 \top F_2$ (en el sentido del apartado 4.º) lo sea también; al contrario, la $\bar{\top}$ definida por la igualdad fundamental

$$F_1 \bar{\top} F_2 = \overline{F_1 \top F_2} \in \mathcal{F}$$

es una ley de composición en la familia de Moore $\mathcal{F}$ de las partes cerradas.

6.º Se llamará *recubrimiento* de un conjunto E toda familia de subconjuntos de E cuya unión sea E . Consideremos ahora una *partición* de un conjunto E , es decir, un recubrimiento de E por subconjuntos no vacíos y dos a dos disjuntos, $C, C', \dots$, llamados *clases*; tenemos pues, designando por $\mathcal{C}$ la familia de las clases,

$$1^\circ E = \bigcup_{C \in \mathcal{C}} C,$$

$$2^\circ C, C' \in \mathcal{C}, C \neq C' \quad \text{implica} \quad C \cap C' = \emptyset.$$

En teoría de conjuntos, se da el nombre de *suma* a toda unión de partes no vacías y disjuntas dos a dos; escribiremos pues, también

$$E = \sum_{C \in \mathcal{C}} C$$

La familia $\mathcal{F} = \mathcal{C} \cup \{\emptyset, E\}$ es visiblemente una familia de Moore. Supongamos ahora que E tenga una ley de composición interna $\top$; en general, en el conjunto $\mathcal{P}(E)$, la familia $\mathcal{F}$ no es estable y el procedimiento del apartado 5.º aplicado a esta familia de Moore da

$$C \bar{\top} C' = E$$

siempre que el conjunto $C \top C'$ no está contenido en una clase única. Pero por el contrario si la partición $\mathcal{C}$ es tal que para cada par C, C' (comprendido el caso $C' = C$), $C \top C'$ está contenido en una sola clase P ($P \in \mathcal{C}$) resulta $C \bar{\top} C' = P$ y en $\mathcal{C}$ se tiene entonces la ley de composición interna $\bar{\top}$.

Es este un caso importante que vamos a encontrar otra vez, en forma distinta.

§ 5. Relaciones de equivalencia compatibles con una ley de composición interna

A la partición $\mathcal{C}$ se asocia una relación $\mathcal{R}$, entre los elementos de E , definida de la forma siguiente: a y a' verifican la relación $\mathcal{R}$, $a\mathcal{R}a'$, si a y a' pertenecen a una misma clase, y sólo en ese caso. Esta relación, $\mathcal{R}$ es reflexiva ($a\mathcal{R}a$ para todo elemento a de E), simétrica ($a\mathcal{R}a'$ implica $a'\mathcal{R}a$) y transitiva ($a\mathcal{R}a'$ y $a'\mathcal{R}a''$ implican $a\mathcal{R}a''$) las relaciones entre los pares de elementos de un conjunto E que poseen las tres propiedades precedentes son llamadas *relaciones de equivalencia*. Se escribe preferentemente $a \equiv a'(\mathcal{R})$ (" a equivalente o congruente con a' , módulo $\mathcal{R}$ "). Así, a toda partición de E va asociada una relación de equivalencia $\mathcal{R}$. El conjunto Q de clases $Q = \{A, B, \dots\} \subseteq \mathcal{P}(E)$ se llama conjunto cociente de E por la equivalencia $\mathcal{R}$; $Q = E/\mathcal{R}$.

Una equivalencia $\mathcal{S}$ está contenida en una equivalencia $\mathcal{R}$, o es más fina que $\mathcal{R}$, $\mathcal{S} \subseteq \mathcal{R}$, si $a \equiv b(\mathcal{S})$ implica $a \equiv b(\mathcal{R})$. La igualdad $\mathcal{E}$ es una equivalencia contenida en toda equivalencia $\mathcal{R}$; toda equivalencia $\mathcal{R}$ está contenida en la equivalencia universal $\mathcal{U}$ (para la cual la partición $\mathcal{C}$ comprende una sola clase, E).

Inversamente a toda relación de equivalencia $\mathcal{R}$ dada *a priori* en E está asociada una partición de E , de tal manera que tenemos $x \equiv y(\mathcal{R})$ si x e y se hallan en la misma clase de esta partición y sólo en ese caso. En efecto a todo elemento x de E asociemos el conjunto $C(x)$ de los elementos x_1 equivalentes a x módulo $\mathcal{R}$; $C(x)$ no es nunca vacío porque, en virtud de la reflexividad de $\mathcal{R}$, $x \in C(x)$ y los $C(x)$ forman un recubrimiento de E . Supongamos

$$C(x) \cap C(x') \neq \emptyset \quad \text{y sea} \quad r \in C(x) \text{ y } r \in C(x');$$

por la simetría de $\mathcal{R}$, tenemos $x' \equiv r(\mathcal{R})$ y por la transitividad, esta relación junto con $r \equiv x(\mathcal{R})$ da $x' \equiv x(\mathcal{R})$; resulta pues, $C(x') = C(x)$, por las propiedades transitiva y simétrica, y los $C(x)$ constituyen efectivamente una partición de E .

Ejemplos de relaciones de equivalencia. — 1) Sea α una aplicación de un conjunto E en un conjunto E' . Se llama *equivalencia de aplicación* asociada a α la equivalencia $\mathcal{R}$ definida en E por $a \equiv b$ si, y sólo si, a y b tienen la misma imagen por α en E' : $\alpha(a) = \alpha(b)$.

2) Sea en el conjunto E' la relación de equivalencia $\mathcal{R}'$ y $\mathcal{C}'$ la correspondiente partición de E' .

Se llama *equivalencia recíproca de $\mathcal{R}'$ por α* , o *alzado de $\mathcal{R}'$ en E con relación a α* , la equivalencia definida en E por la partición cuyas clases son las imá-

genes¹ de las clases de $\mathcal{C}'$ por la aplicación recíproca de α .

La designaremos por $\mathcal{R}'_{\alpha^{-1}}$. Se tiene pues

$$a \equiv b (\mathcal{R}'_{\alpha^{-1}}) \quad \text{si, y sólo si,} \quad \alpha(a) \equiv \alpha(b) (\mathcal{R}').$$

Si $\mathcal{E}'$ es la igualdad en E' , para la equivalencia de aplicación $\mathcal{R}$ se tiene evidentemente

$$\mathcal{R} = \mathcal{E}'_{\alpha^{-1}}$$

y así mismo

$$\mathcal{R} \subseteq \mathcal{R}'_{\alpha^{-1}}$$

para toda equivalencia $\mathcal{R}'$ definida en E' .

Por ejemplo, supongamos que E y E' son dos planos perpendiculares (fig. 2), considerados como conjunto de sus puntos, y que α sea la proyección ortogonal h sobre E' ; $h(E)$ es la recta

$$\Delta = E \cap E';$$

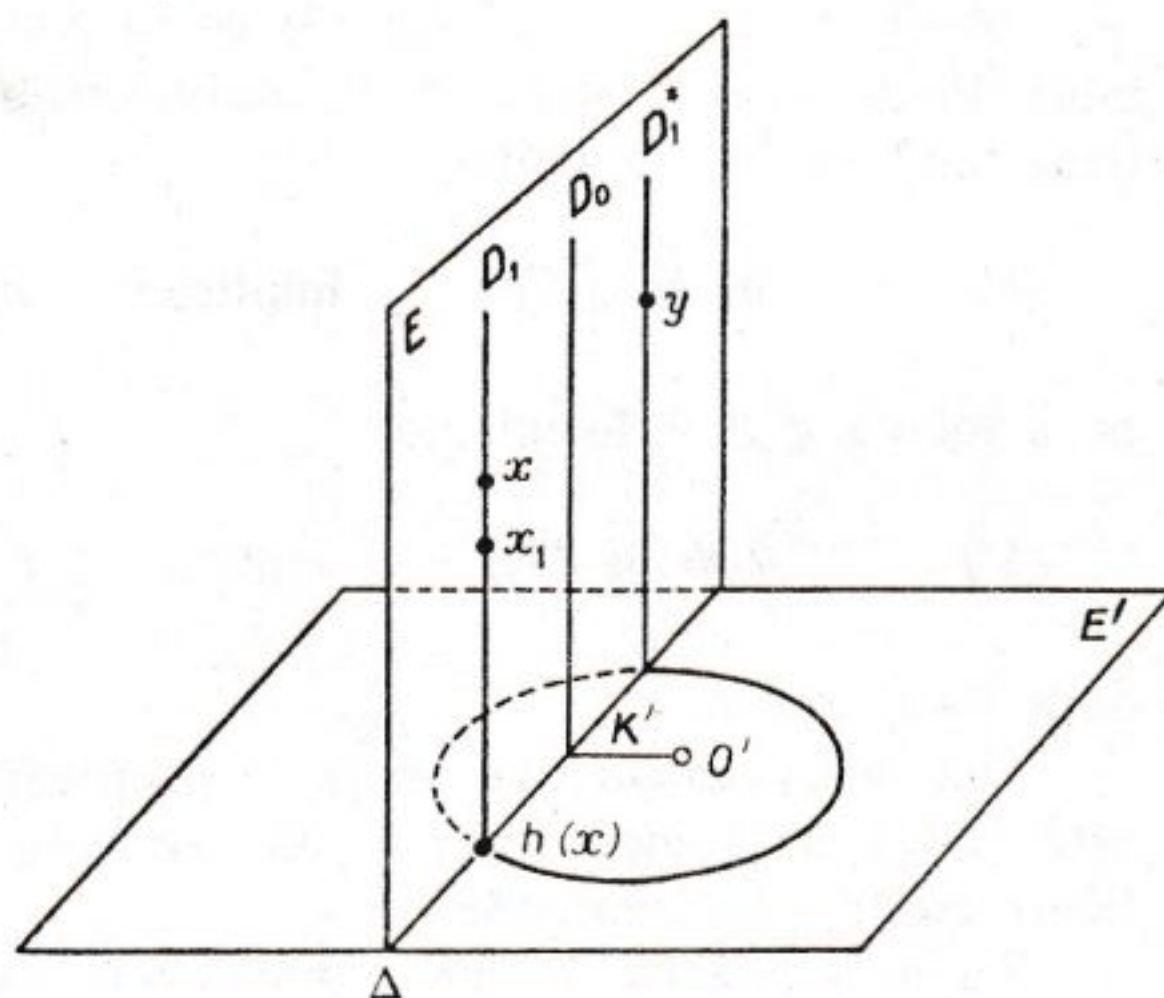


FIG. 2.

dos puntos x, x_1 de E son equivalentes módulo $\mathcal{R}$ si están sobre una misma perpendicular a Δ . Tomemos para $\mathcal{R}'$ la equivalencia siguiente: dos puntos x', x'_1 de E' verifican la relación $\mathcal{R}'$ si están a la misma distancia de un punto O' fijo, de E' . El alzado de $\mathcal{R}'$ es la relación $\mathcal{R}'_{h^{-1}}$ definida así: dos puntos x, y de E verifican $\mathcal{R}'_{h^{-1}}$ si están sobre un mismo cilindro de revolución que tenga por eje la perpendicular a E' en O' ; si D_0 es la perpendicular a E' por la proyección K' de O' sobre Δ , las clases de equivalencia módulo $\mathcal{R}'_{h^{-1}}$ son: una D_0 ; las otras, los pares de rectas D_1, D_1^* del plano E equidistantes de D_0 .

Supongamos ahora que E es un conjunto con la ley de composición interna $\mathcal{T}$. Es fácil de caracterizar el caso en el que se puede definir a partir de la ley $\mathcal{T}$ de E una ley de composición $\bar{\mathcal{T}}$ en el conjunto cociente $\mathcal{C} = E/\mathcal{R}$. Ese caso, como hemos visto antes, es aquel en que $C \mathcal{T} C' = \{a \mathcal{T} a', a \in C, a' \in C'\}$ está contenido en una sola clase P , y esto cualesquiera que sean $C, C' \in \mathcal{C}$. Ahora

¹ La imagen A' de un subconjunto A de E en la aplicación α de E en E' es naturalmente la unión de las imágenes de todos los elementos de A . La imagen recíproca $\alpha^{-1}(A')$ es el conjunto de todos los elementos de E cuyas imágenes por α están en A' : $\alpha^{-1}(A') \supseteq A$.

bien, esta propiedad se cumple al mismo tiempo que la siguiente:

$$(3) \quad a_1 \equiv a (\mathcal{R}) \text{ y } a'_1 \equiv a' (\mathcal{R}) \text{ implica } a_1 \top a'_1 \equiv a \top a' (\mathcal{R}).$$

Una equivalencia $\mathcal{R}$ que verifica la condición (3) se dice *compatible* con la ley de composición de E . Por lo anteriormente dicho, esta compatibilidad es una condición necesaria y suficiente para poder hablar de la ley de composición interna $\bar{\top}$ asociada en el conjunto cociente $E/\mathcal{R}$. Esta ley está, pues, definida por

$$C \bar{\top} C' \in \mathcal{C}; \quad C \bar{\top} C' \geq C \top C'.$$

Ahora bien, la condición (3) es la conjunción de dos condiciones más débiles. Pues como la relación de equivalencia $\mathcal{R}$ es reflexiva, si (3) se verifica, se tiene también la propiedad:

$$(4) \quad a_1 \equiv a (\mathcal{R}) \quad \text{implica} \quad a_1 \top x \equiv a \top x (\mathcal{R})$$

para todo $x \in E$ y, lo mismo:

$$(4') \quad a \equiv a_2 (\mathcal{R}) \quad \text{implica} \quad x \top a \equiv x \top a_2 (\mathcal{R})$$

para todo $x \in E$.

Una equivalencia que tenga la propiedad (4) se llama *regular a la derecha* para la ley de composición $\top$; una equivalencia que tenga la propiedad (4') se dice *regular a la izquierda*.

Recíprocamente, si una equivalencia es *regular*, es decir, simultáneamente *regular a la derecha* y *regular a la izquierda*, con relación a $\top$, y si tenemos

$$a_1 \equiv a \quad \text{y} \quad b_1 \equiv b \quad (\mathcal{R})$$

entonces se deduce que

$$a_1 \top b_1 \equiv a \top b_1 \quad \text{y} \quad a \top b_1 \equiv a \top b \quad (\mathcal{R})$$

de donde

$$a_1 \top b_1 \equiv a \top b \quad (\mathcal{R})$$

y $\mathcal{R}$ es compatible con la ley de composición de E ; las *dos propiedades de compatibilidad y de regularidad se implican mutuamente*.

Ejemplo 1. Equivalencia de clausura de Moore. — A una clausura de Moore $A \rightarrow \bar{A}$ definida en el conjunto $\mathcal{P}(E)$ de las partes de E , se puede asociar una

relación de equivalencia $\mathcal{R}$ definida así,

$$A \equiv A_1 (\mathcal{R}) \quad \text{si} \quad \bar{A} = \bar{A}_1$$

a la que llamaremos *equivalencia de clausura*. Cada parte A_1 de E que tiene la misma clausura de Moore $\bar{A}$ que A , se llama, por definición, un *sistema de generadores* de $\bar{A}$. Los diversos sistemas de generadores $A, A_1, \dots$ tienen evidentemente un elemento *máximo* $\bar{A}$ (con respecto a la inclusión). Si en el conjunto $\{A, A_1, \dots, \bar{A}\}$ existen elementos *minorantes*, esto es que no incluyen a ningún otro, cada uno de estos se llama *sistema mínimo* (o *irreducible*) de generadores; y se dice, también, que es un sistema de generadores sin *elementos superfluos*. Todo subconjunto propio S de un tal sistema mínimo tiene una clausura $\bar{S}$ estrictamente contenida en $\bar{A}$.

Lema. *Se tienen las relaciones:*

$$\overline{A \cup B} = \overline{\bar{A} \cup B} = \overline{A \cup \bar{B}} = \overline{\bar{A} \cup \bar{B}}.$$

En efecto de las inclusiones $A \subseteq \bar{A}$, $B \subseteq \bar{B}$ se deduce

$$A \cup B \subseteq \bar{A} \cup B \subseteq \bar{A} \cup \bar{B}$$

de donde

$$\overline{A \cup B} \subseteq \overline{\bar{A} \cup B} \subseteq \overline{\bar{A} \cup \bar{B}}$$

y por lo mismo

$$\overline{A \cup B} \subseteq \overline{A \cup \bar{B}} \subseteq \overline{\bar{A} \cup \bar{B}}.$$

Por otra parte, de $A \subseteq A \cup B$ y $B \subseteq A \cup B$ se deduce

$$\bar{A} \subseteq \overline{A \cup B}, \quad \bar{B} \subseteq \overline{A \cup B}$$

de donde

$$\bar{A} \cup \bar{B} \subseteq \overline{A \cup B},$$

luego

$$\overline{\bar{A} \cup \bar{B}} \subseteq \overline{A \cup B}.$$

Así quedan establecidas las igualdades del enunciado.

Consecuencias. — a) Para tres partes A, B, C de E , se tiene

$$\overline{A \cup B \cup C} = \overline{\overline{A} \cup \overline{B} \cup \overline{C}}$$

y así sucesivamente.

b) **Teorema 2.** — La equivalencia de clausura es regular para la unión de partes:

$$A \equiv A_1 \quad (\mathcal{R}) \quad \text{implica} \quad A \cup X \equiv A_1 \cup X \quad (\mathcal{R})$$

cualquiera que sea $X \in \mathcal{P}(E)$.

Tenemos por hipótesis $\overline{A} = \overline{A_1}$ de donde en virtud del lema

$$\overline{A \cup X} = \overline{\overline{A} \cup X} = \overline{\overline{A_1} \cup X} = \overline{A_1 \cup X}$$

es decir, $A \cup X \equiv A_1 \cup X \quad (\mathcal{R})$.

Ejemplo 2. — Sean E un conjunto y $\mathcal{R}$ una equivalencia en E . Sea E' un subconjunto de E . A la partición $\mathcal{C}$ de E asociada a $\mathcal{R}$ corresponde en E' la partición $\mathcal{C}'$ formada de las $E' \cap C = C'$ para todas las clases C que tienen con E' una intersección no vacía. Tenemos aquí una partición de E' , porque todo elemento e' de E' pertenece a una clase, y una sola, de $\mathcal{C}$.

La relación de equivalencia $\mathcal{R}'$ definida por esta partición $\mathcal{C}'$ de E' , se llama *restricción de $\mathcal{R}$ a E'* .

Si E' es una parte estable y si la equivalencia $\mathcal{R}$ es regular con relación a la ley de composición definida en E , evidentemente será lo mismo para $\mathcal{R}'$, restricción de $\mathcal{R}$ a E' .

Ejemplo 3. Congruencias aritméticas. Consideremos el conjunto $\mathbf{Z}$ de los enteros relativos (es decir positivos, negativos o nulos). Dado un entero positivo m llamado *módulo*, la *congruencia aritmética módulo m* es, por definición, la relación $\mathcal{C}_m$ definida en $\mathbf{Z}$ por

$$x \mathcal{C}_m y \quad \text{si} \quad x - y = km,$$

con $k \in \mathbf{Z}$.

Se dice entonces que x e y son *congruentes módulo m* , y se escribe también

$$x \equiv y \quad (m)$$

Esta propiedad significa que x e y , divididos por m , dan el *mismo resto*.

La relación C_m es reflexiva, simétrica y transitiva; es una *relación de equivalencia*. Las clases de equivalencia son las diferentes progresiones aritméticas de razón m , ilimitadas en los dos sentidos:

$$\begin{aligned} & \dots, -m, 0, m, 2m, \dots \\ & \dots, -m+1, 1, m+1, 2m+1, \dots \\ & \dots, -1, m-1, 2m-1, 3m-1, \dots \end{aligned}$$

Estas se corresponden biunívocamente con los m valores posibles, $0, 1, \dots, m-1$ del resto de un entero x por el módulo m . Se les llama *clases residuales módulo m* ; las designaremos por $\bar{0}, \bar{1}, \dots, \overline{m-1}$ ó $0, 1, \dots$ etc. El conjunto cociente $\mathbf{Z}/C_m$, llamado *conjunto de clases residuales módulo m* es designado más sencillamente por $\mathbf{Z}/(m)$.

Como se ve inmediatamente, *la congruencia aritmética es regular con relación a la adición y multiplicación de enteros*. El procedimiento visto más arriba permite pues definir en el conjunto $\mathbf{Z}/(m)$ de clases residuales, una adición y una multiplicación; se determina prácticamente la suma o el producto de dos clases, sumando o multiplicando dos números de estas clases, con preferencia los restos que las representan, y reemplazando luego el resultado por el resto de su división por m .

Se obtienen así, por ejemplo, las siguientes tablas de adición y multiplicación para el conjunto de clases residuales módulo 6:

+	0	1	2	3	4	5			0	1	2	3	4	5
0	0	1	2	3	4	5	0	0	0	0	0	0	0	0
1	1	2	3	4	5	0	1	0	1	2	3	4	5	
2	2	3	4	5	0	1	2	0	2	4	0	2	4	
3	3	4	5	0	1	2	3	0	3	0	3	0	3	
4	4	5	0	1	2	3	4	0	4	2	0	4	2	
5	5	0	1	2	3	4	5	0	5	4	3	2	1	

Observación. — Se puede también considerar la restricción de esta equivalencia al conjunto $\mathbf{N}$ de los enteros naturales. Como $\mathbf{N} \cap C$ no es vacío para ninguna clase C , los conjuntos $\mathbf{Z}/(m)$ y $\mathbf{N}/(m)$ se corresponden biyectivamente y

pueden ser identificados. Habríamos podido introducir directamente esta equivalencia en el conjunto $\mathbf{N}$ de enteros naturales definiendo

$$x \equiv y (m)$$

si, y sólo si, $|x - y| = km$, donde k es un entero positivo o cero.

§ 6. Aplicaciones notables de un conjunto con una ley de composición interna en o sobre otro: homomorfismos; isomorfismos

Para más comodidad, utilizaremos en lo que sigue los cuantificadores $\forall$, que se lee “para todo”, o “cualquiera que sea”, y $\exists$ “existe al menos un”.

Consideremos los dos conjuntos: E , con la ley de composición $\mathbf{T}$, y E' con la ley de composición $\mathbf{T}'$.

Diremos que una aplicación h de E en E' respeta las leyes de composición $\mathbf{T}$ y $\mathbf{T}'$, o que es *compatible* con estas leyes o también, que es un *homomorfismo* de E en E' si se tiene

$$(1) \quad h(x \mathbf{T} y) = h(x) \mathbf{T}' h(y) \quad \forall x, y \in E.$$

Si, como sucede frecuentemente, las dos leyes $\mathbf{T}$ y $\mathbf{T}'$ se indican por medio de un mismo símbolo, por ejemplo $+$ ó $\cdot$, la condición (1) se escribe

$$(1') \quad h(x + y) = h(x) + h(y) \quad \forall x, y \in E$$

$$(1'') \quad h(x \cdot y) = h(x) \cdot h(y) \quad \forall x, y \in E$$

y se enuncia: la imagen de una suma de elementos de E es la suma, en E' , de sus imágenes; la imagen de un producto de elementos de E es el producto, en E' , de sus imágenes.

Se escribe

$$(h) \quad E \rightarrow E' \quad \text{o} \quad E \xrightarrow{h} E'$$

y se dice que el homomorfismo h aplica E en E' .

Al conjunto $\overline{E}$ de los elementos $\bar{x}$ de E' que son la imagen por h de al menos un elemento x de E :

$$\overline{E} = \{ \bar{x}; \bar{x} \in E', \exists x \in E \text{ tal que } h(x) = \bar{x} \},$$

designado también por $h(E)$, se le llama *imagen homomorfa* de E .

Teorema 1. — *La imagen homomorfa $\bar{E} = h(E)$ es una parte estable de E' . Sean $\bar{x}, \bar{y} \in \bar{E}$; existen en E elementos x, y tales que*

$$h(x) = \bar{x}, \quad h(y) = \bar{y}.$$

Tenemos por (1),

$$h(x \top y) = \bar{x} \top' \bar{y}$$

luego $\bar{x} \top' \bar{y} \in \bar{E}$, como se quería demostrar.

En virtud del teorema 1, podremos hablar de la restricción de $\top'$ a $\bar{E}$ (§ 4, 3.º).

Un caso particular importante es aquel en que $\bar{E} = E'$, en otros términos, el caso en que h es una aplicación *exhaustiva*; se dice entonces que h , que cumple por hipótesis la condición (1), es un homomorfismo que aplica E sobre E' (o un *epimorfismo*), y se escribe

$$(h) \quad E \sim E' \quad \text{o} \quad E \sim E' = h(E).$$

El caso general puede reducirse a éste, reemplazando h por la aplicación $\bar{h}$ de E sobre $\bar{E} = h(E)$ definida por

$$\bar{h}(x) = h(x), \quad \forall x \in E.$$

Ahora si $\mathfrak{E}$ designa la aplicación idéntica de $\bar{E}$ en E'

$$\mathfrak{E}(\bar{x}) = \bar{x} \quad \forall \bar{x} \in \bar{E},$$

se tiene

$$h = \mathfrak{E} \circ \bar{h}$$

El estudio de h se reduce así al de $\bar{h}$.

Otro caso notable es aquel en que el homomorfismo h es una aplicación *inyectiva* ($x \neq y$ implica $h(x) \neq h(y)$); entonces ocurrirá lo mismo con $\bar{h}$, que es por consiguiente una aplicación biyectiva de E sobre $\bar{E}$ conservando las leyes de composición $\top$ de E , y $\top'$ de $\bar{E}$. Decimos entonces que h es un *isomorfismo* que aplica E sobre $\bar{E}$, y también que E es *isomorfo* a $\bar{E}$. Designando el isomorfismo

por i , $h = i$, esto se escribirá así:

$$(i) \quad E \simeq \overline{E} = i(E).$$

Sea entonces i^{-1} la aplicación inversa o recíproca de i , esto es la que asocia a cada elemento $\bar{x}$ de $\overline{E}$ el elemento único x tal que $i(x) = \bar{x}$, $x = i^{-1}(\bar{x})$; tomando la imagen según i^{-1} de la igualdad

$$(1) \quad i(x \top y) = [i(x)] \top' [i(y)]$$

obtendremos

$$x \top y = i^{-1} [(i(x)) \top' (i(y))]$$

es decir

$$[i^{-1}(\bar{x})] \top [i^{-1}(\bar{y})] = i^{-1}[\bar{x} \top' \bar{y}].$$

Vemos así que i^{-1} es también un isomorfismo que aplica $\overline{E}$ sobre E ; es el *isomorfismo inverso* o *recíproco* de i ; $i^{-1} \circ i$ es la aplicación idéntica de E sobre E , $i \circ i^{-1}$ es la aplicación idéntica de $\overline{E}$ sobre $\overline{E}$.

Todo lo que precede se aplica, desde luego, cuando E' coincide con E y cuando la ley de composición $\top'$ coincide con $\top$: un homomorfismo de E en E es lo que se llama un *endomorfismo* de E ; un isomorfismo de E sobre E es lo que se llama un *automorfismo* de E .

Ejemplos. — 1. Para toda parte estable E de E' , la aplicación idéntica ξ de E sobre sí mismo:

$$\xi(x) = x \quad \forall x \in E$$

es un homomorfismo de E en E' :

$$(\xi) \quad E \rightarrow E'.$$

Se tiene aquí $\overline{E} = \xi(E) = E$.

En particular, la aplicación idéntica de E' sobre sí mismo es un automorfismo de E' , llamado *automorfismo idéntico*.

2. Asociemos a todo número real positivo el número $+1$, a todo número real negativo el número -1 ; definimos así una aplicación h del conjunto $\mathbf{R}^*$

de los reales no nulos en el conjunto $S = \{-1, +1\}$. Tomemos además como ley de composición en $\mathbf{R}^*$ la multiplicación; S es entonces una parte estable de $\mathbf{R}^*$ y h es un homomorfismo que aplica $\mathbf{R}^*$ sobre S . Esta propiedad traduce en cierto modo la "regla de los signos".

3. Para el conjunto $\mathbf{Z}$ de los enteros relativos, *con la adición*, la aplicación

$$(\alpha) \quad x \rightarrow -x$$

es un *automorfismo*; no lo es si se cambia la adición por la multiplicación
La aplicación

$$(\beta) \quad x \rightarrow 2x, \quad x \in \mathbf{Z}$$

es un isomorfismo que aplica el conjunto aditivo $\mathbf{Z}$ sobre el conjunto aditivo $\mathbf{Z}'$ de los enteros pares (≥ 0); es un endomorfismo de $\mathbf{Z}$ (además inyectivo), pero no es un automorfismo.

La aplicación

$$(\beta') \quad x \rightarrow 2x, \quad x \in \mathbf{Q}$$

es un *automorfismo* del conjunto aditivo $\mathbf{Q}$ de los números *racionales*.

4. Consideremos un número real $a > 0$. La aplicación (o función) exponencial

$$(f) \quad x \rightarrow a^x, \quad x \in \mathbf{R}$$

es un *homomorfismo* que aplica el conjunto aditivo $\mathbf{R}$ en el conjunto multiplicativo $\mathbf{R}^+$ (conjunto de los reales positivos); se tiene en efecto

$$a^{x+y} = a^x \cdot a^y$$

Si $a \neq 1$, se tiene $f(\mathbf{R}) = \mathbf{R}^+$ y f es inyectiva: f es un *isomorfismo*. No ocurre lo mismo si $a = 1$, puesto que entonces $f(\mathbf{R}) = \{1\}$.

5. Consideremos dos planos P y P' , y los conjuntos E , E' de los vectores (libres) de P y de P' , con la adición geométrica de estos vectores como ley de composición. Al asociar a cada vector x de P su proyección ortogonal x' sobre P' , definiremos una aplicación π de E en E' que es:

un *isomorfismo* de E sobre E' si P y P' no son perpendiculares;

un *homomorfismo* de E en E' si P y P' son perpendiculares: $\pi(E) = \overline{E}$ es

entonces el conjunto de vectores que tienen como soporte la recta intersección P y P' .

Las proyecciones (ortogonales u oblicuas) de los vectores del espacio sobre los planos o sobre las rectas son *endomorfismos* del conjunto V de los vectores del espacio, con la suma geométrica como ley de composición. La relación fundamental:

$$\pi(x + y) = \pi(x) + \pi(y)$$

expresa el "teorema de las proyecciones",

6. Sea $\mathcal{R}$ una equivalencia regular en un conjunto E , con ley de composición $\top$. Hemos definido en el conjunto de las clases o conjunto cociente $E/\mathcal{R}$ la ley de composición designada por $\bar{\top}$, conviniendo que $X \bar{\top} Y$ es la clase que contiene $x \top y$, donde $x \in X$ e $y \in Y$. Es decir que la *aplicación canónica* f de E sobre $E/\mathcal{R}$ que asocia a cada elemento x de E , la clase X módulo $\mathcal{R}$ que contiene a x , es un *homomorfismo*, llamado *natural* o *canónico*; escribiremos

$$E \sim E/\mathcal{R} \quad \text{o} \quad (f) \quad E \rightarrow E/\mathcal{R}$$

A un homomorfismo cualquiera

$$(h) \quad E \rightarrow E'$$

o, lo que es lo mismo, al homomorfismo correspondiente $\bar{h}$ de E sobre $\bar{E} = h(E)$,

$$(\bar{h}) \quad E \sim \bar{E} = h(E)$$

asociemos la equivalencia de homomorfismo $\mathcal{R}$: es decir, la equivalencia de la aplicación ya introducida que se define, en E , por:

$$a_1 \equiv a_2 (\mathcal{R}) \quad \text{si} \quad \bar{h}(a_1) = \bar{h}(a_2) \quad (\text{o} \quad h(a_1) = h(a_2)).$$

Teorema 2. — *La equivalencia de homomorfismo $\mathcal{R}$ es compatible con la ley de composición $\top$ de E .*

Veamos que $\mathcal{R}$ es regular por ambos lados, y para eso, por ejemplo que es regular a la derecha. Si $a_1 \equiv a_2 (\mathcal{R})$, es decir, $\bar{h}(a_1) = \bar{h}(a_2)$, se tiene para todo $x \in E$,

$$\bar{h}(a_1 \top x) = [\bar{h}(a_1)] \top' [\bar{h}(x)] = [\bar{h}(a_2)] \top' [\bar{h}(x)] = \bar{h}(a_2 \top x)$$

luego

$$a_1 \top x \equiv a_2 \top x \quad (\mathcal{R}), \quad \forall x \in E.$$

Consideremos ahora el conjunto cociente $E/\mathcal{R}$, con su ley de composición de clases (definida a partir de $\top$ y designada también por $\top$); asociemos a cada elemento $\bar{x}$ de $\bar{E}$ el conjunto (no vacío) X de los elementos x de E que tienen por imagen $\bar{x}$: $X = \{x; x \in E, h(x) = \bar{x}\}$. X es una clase módulo $\mathcal{R}$: $X \in E/\mathcal{R}$, y obtenemos de este modo una aplicación *biyectiva* i de $\bar{E}$ sobre $E/\mathcal{R}$

$$(i) \quad \bar{x} \rightarrow X = i(\bar{x}) \quad (\bar{x} = \bar{h}(x) \text{ y } x \in X).$$

Además, i respeta las operaciones, pues, si $\bar{y} = \bar{h}(y)$ e $y \in Y$, se tiene por una parte:

$$\bar{x} \top' \bar{y} = [\bar{h}(x)] \top' [\bar{h}(y)] = \bar{h}[x \top y]$$

y por otra parte (por la definición de la ley $\top$ en $E/\mathcal{R}$)

$$x \top y \in X \top Y$$

luego, según la definición de i ,

$$i(\bar{x} \top' \bar{y}) = X \top Y = [i(\bar{x})] \top [i(\bar{y})].$$

Por consiguiente, i es un *isomorfismo* y podemos enunciar:

Teorema 3 (teorema del homomorfismo). — *Todo homomorfismo $\bar{h}$ que aplica E sobre $\bar{E}$:*

$$(\bar{h}) \quad E \sim \bar{E} = h(E)$$

implica, designando por $\mathcal{R}$ la equivalencia de homomorfismo correspondiente, el isomorfismo

$$(i) \quad \bar{E} \simeq E/\mathcal{R},$$

en el que

$$i(\bar{x}) = X = \{x; \bar{h}(x) = \bar{x}\}.$$

Corolario. — *Para todo homomorfismo*

$$(h) \quad E \rightarrow E'$$

se tiene la descomposición canónica:

$$h = \epsilon \circ i^{-1} \circ f$$

en la que f es el homomorfismo canónico que aplica E sobre $E/\mathcal{R}$, $\mathcal{R}$ designa la equivalencia del homomorfismo ($x \equiv y(\mathcal{R})$ si $h(x) = h(y)$), i^{-1} el isomorfismo $E/\mathcal{R} \simeq \bar{E}$ inverso de i , y ϵ la aplicación idéntica de $\bar{E}$ sobre sí mismo en E' .

Teorema 4. — Si h es un homomorfismo de E en E' y h' un homomorfismo de E' en E'' , la aplicación compuesta $f = h' \circ h$ es un homomorfismo de E en E'' .

La aplicación compuesta $f = h' \circ h$ aplica E en E'' . Tenemos, además al designar por $\top$, $\top'$, $\top''$ las leyes de composición respectivas de E , E' , E'' , y por x , y dos elementos cualesquiera de E :

$$\begin{aligned} f(x \top y) &= h'[h(x \top y)] = h'[(h(x)) \top' (h(y))] \\ &= [h'(h(x))] \top'' [h'(h(y))] = [f(x)] \top'' [f(y)]. \end{aligned}$$

La aplicación f es pues efectivamente un homomorfismo que aplica E en E'' .

Si h es un homomorfismo que aplica E sobre E' y h' un homomorfismo que aplica E' sobre E'' , el homomorfismo f aplica E sobre E'' .

De modo general tenemos,

$$f(E) = h'[h(E)]$$

Apliquemos el teorema del homomorfismo (teorema 3). Tenemos:

$$f(E) \simeq E/\rho,$$

donde ρ designa la equivalencia de homomorfismo definida en E , asociada a f :

$$x \equiv y(\rho) \quad \text{si y sólo si} \quad f(x) = f(y) \quad (x, y \in E).$$

Puesto que $f = h' \circ h$, tenemos

$$x \equiv y(\rho) \quad \text{si y sólo si} \quad h(x) \equiv h(y) \quad (\rho')$$

designando por ρ' la equivalencia definida en E' asociada al homomorfismo $h'(x' \equiv y'(\rho')$ si y sólo si $h'(x') = h'(y')$). Por lo tanto ρ es el alzado de ρ' en E , con relación a h , y tenemos:

$$\mathcal{R} \subseteq \rho.$$

Podemos finalmente considerar E , E' y h fijos y tomar como ρ' no importa qué equivalencia definida en E' y compatible con la ley de composición T' ; h' será entonces el homomorfismo canónico que aplica E' sobre el conjunto cociente E'/ρ' que desempeña el papel de E'' :

Resumiendo, podemos enunciar el teorema que sigue:

Teorema 5 (primer teorema del isomorfismo). — 1.º Dado un homomorfismo compuesto

$$f = h' \circ h, \quad \text{donde} \quad h : E \rightarrow E' \quad \text{y} \quad h' : E' \rightarrow E'',$$

se tiene

$$f(E) \simeq E/\rho$$

donde ρ es el alzado en E , con relación a h , de la equivalencia regular ρ' asociada en E' al homomorfismo h' ; se tiene: $\mathcal{R} \subseteq \rho$, donde $\mathcal{R}$ designa la equivalencia de homomorfismo asociada a h .

2.º El alzado ρ en E , con relación a h , de una equivalencia ρ' definida en E' y compatible con la ley de composición T' de E' es la equivalencia asociada, en E , al homomorfismo compuesto $f = h' \circ h$, donde h' designa el homomorfismo canónico $E' \sim E'/\rho'$; por consiguiente ρ es compatible con la ley de composición T de E .

§ 7. Elementos notables de un conjunto con una ley de composición interna

Sea E un conjunto con una ley de composición T .

Un elemento a de E se llama *simplificable a la izquierda*, cuando la igualdad

$$a \mathbin{T} x = a \mathbin{T} y \quad (x, y \in E) \quad \text{implica} \quad x = y$$

o, dicho de otro modo cuando $x \neq y$ implica $a \mathbin{T} x \neq a \mathbin{T} y$. Si E es finito la propiedad precedente significa que en la tabla E , la fila correspondiente al elemento a no contiene repetido ningún elemento de E ; por consiguiente, cada elemento de E aparecerá una vez, y sólo una, en dicha fila.

Se define de una manera análoga un elemento *simplificable a la derecha*. Si E es finito, la columna correspondiente de la tabla contiene una vez, y sólo una, a cada elemento de E . Inversamente, esta circunstancia en una columna de la tabla significa que el elemento correspondiente es simplificable a la derecha.

Se llama *simplificable*, sin más, todo elemento simplificable a la derecha y a la izquierda. Como sinónimo de simplificable, se dice también que el elemento es *cancelable* o *regular*.

Diremos que E verifica la *regla de simplificación a la izquierda (derecha)* si todo elemento de E es simplificable a la izquierda (derecha); y diremos que E verifica la *regla de simplificación* (o *cancelativa*) si todo elemento de E es simplificable o regular. En este caso se dice, también, que E es un *conjunto regular*.

Ejemplos. — El conjunto *aditivo* $\mathbf{Z}$ de los enteros relativos verifica la regla de simplificación. No es lo mismo si la ley de composición considerada en $\mathbf{Z}$ es la multiplicación de los enteros: en este caso, 0 no es simplificable. El conjunto $\mathbf{N}$ de los enteros naturales, cuando la ley de composición sea la adición (o la multiplicación) verifica la regla de simplificación. No sería lo mismo si se tomase como operación la formación del m.c.d. o del m.c.m.

Un elemento a de E se dice *idempotente* si verifica la igualdad

$$a \mathbin{\mathsf{T}} a = a.$$

En $\mathbf{Z}$, con la multiplicación como ley de composición los números 0 y 1 son idempotentes. En el conjunto multiplicativo $\mathbf{Z}/(6)$ los elementos idempotentes son las clases 0, 1, 3, 4.

Si *todo* elemento de E es idempotente, tanto la *ley de composición* como el propio conjunto E se llaman *idempotentes*. Con la formación de la media aritmética como ley de composición, $x \mathbin{\mathsf{T}} y = \frac{x+y}{2}$; el conjunto $\mathbf{Q}$ de los números racionales es idempotente; y también lo es $\mathbf{N}$ por la formación del m.c.d. o del m.c.m.

Elementos idempotentes particulares, muy importantes, son los *elementos lícitos* y los *elementos neutros*.

Un elemento z de E se llama *lícito a la derecha* para la operación T , si

$$z \mathbin{\mathsf{T}} x = z, \quad \forall x \in E.$$

En particular, se tiene $z \mathbin{\mathsf{T}} z = z$; todo elemento lícito a la derecha es idempotente. De manera análoga se define un elemento z' *lícito a la izquierda*; elemento *lícito* se llama al que lo es simultáneamente a la derecha y a la izquierda.

En cualquier conjunto E existe a lo más un elemento lícito. En efecto, si z es lícito a la derecha y z' lícito a la izquierda, tenemos $z \mathbin{\mathsf{T}} z' = z$, y $z \mathbin{\mathsf{T}} z' = z'$, de donde $z = z'$. Hemos encontrado, en el § 3, ejemplo 1, un caso donde todo elemento $a_i (i = 1, 2, 3)$ es lícito a la izquierda.

Podemos finalmente considerar E , E' y h fijos y tomar como ρ' no importa qué equivalencia definida en E' y compatible con la ley de composición T' ; h' será entonces el homomorfismo canónico que aplica E' sobre el conjunto cociente E'/ρ' que desempeña el papel de E'' :

Resumiendo, podemos enunciar el teorema que sigue:

Teorema 5 (primer teorema del isomorfismo). — 1.º Dado un homomorfismo compuesto

$$f = h' \circ h, \quad \text{donde} \quad h : E \rightarrow E' \quad \text{y} \quad h' : E' \rightarrow E'',$$

se tiene

$$f(E) \simeq E/\rho$$

donde ρ es el alzado en E , con relación a h , de la equivalencia regular ρ' asociada en E' al homomorfismo h' ; se tiene: $\mathcal{R} \subseteq \rho$, donde $\mathcal{R}$ designa la equivalencia de homomorfismo asociada a h .

2.º El alzado ρ en E , con relación a h , de una equivalencia ρ' definida en E' y compatible con la ley de composición T' de E' es la equivalencia asociada, en E , al homomorfismo compuesto $f = h' \circ h$, donde h' designa el homomorfismo canónico $E' \sim E'/\rho'$; por consiguiente ρ es compatible con la ley de composición T de E .

§ 7. Elementos notables de un conjunto con una ley de composición interna

Sea E un conjunto con una ley de composición T .

Un elemento a de E se llama *simplificable a la izquierda*, cuando la igualdad

$$a \ T \ x = a \ T \ y \quad (x, y \in E) \quad \text{implica} \quad x = y$$

o, dicho de otro modo cuando $x \neq y$ implica $a \ T \ x \neq a \ T \ y$. Si E es finito la propiedad precedente significa que en la tabla E , la fila correspondiente al elemento a no contiene repetido ningún elemento de E ; por consiguiente, cada elemento de E aparecerá una vez, y sólo una, en dicha fila.

Se define de una manera análoga un elemento *simplificable a la derecha*. Si E es finito, la columna correspondiente de la tabla contiene una vez, y sólo una, a cada elemento de E . Inversamente, esta circunstancia en una columna de la tabla significa que el elemento correspondiente es simplificable a la derecha.

en cuyo caso se dice que a'' es un *inverso de a a la izquierda con relación a e* . Si a' y a'' existen simultáneamente, se dice que a es *invertible*. Un elemento a *simplificable a la izquierda admite, a lo más, un inverso a la derecha*.

Cuando e es neutro (a los dos lados) y para un elemento a de E , existe un mismo elemento a^* verificando las dos igualdades

$$a \top a^* = a^* \top a = e$$

se dice que a y a^* son *simétricos*, y que a es *simetrizable*. Todo elemento simetrizable es pues, invertible. Naturalmente, todo elemento regular posee a lo más un simétrico. Esto mismo ocurre en el caso de toda ley asociativa (cap. II, § 1, torema 9). Cuando un elemento simetrizable a tiene *solamente un simétrico a^** , se dice que a^* es *el simétrico de a* . En notación aditiva, el simétrico de a toma el nombre de *elemento opuesto* y se indica $-a$; en notación multiplicativa, el simétrico se llama *elemento inverso* y se designa por a^{-1} .

Un elemento a que es su propio simétrico, $a \top a = e$, se llama *involutivo*; el elemento neutro e tiene esa propiedad.

Teorema 1. — Sea $\overline{E}$ un conjunto con ley de composición $\overline{\top}$, imagen homomorfa de un conjunto E con ley de composición $\top$:

$$(h) \quad E \sim \overline{E} = h(E).$$

1.º La imagen $\overline{a} = h(a)$ de un elemento idempotente a de E es un elemento idempotente de $\overline{E}$.

2.º La imagen $\overline{z} = h(z)$ de un elemento z de E lícito a la izquierda (por ejemplo), es un elemento lícito a la izquierda de $\overline{E}$.

3.º La imagen $\overline{e} = h(e)$ de un elemento neutro e a la izquierda es un elemento neutro a la izquierda de $\overline{E}$.

4.º La imagen $\overline{a''} = h(a'')$ de un inverso a la izquierda a'' con relación a e es un inverso a la izquierda de la imagen $\overline{a} = h(a)$ con relación a la imagen $\overline{e} = h(e)$.

Demostraciones. — 1.º Tenemos por hipótesis $a \top a = a$, de donde $h(a \top a) = h(a) = \overline{a}$ pero $h(a \top a) = \overline{a} \overline{\top} \overline{a}$, por consiguiente $\overline{a} \overline{\top} \overline{a} = \overline{a}$.

2.º Un elemento cualquiera $\overline{x}$ de $\overline{E}$ es la imagen de al menos un elemento x de E : $\overline{x} = h(x)$. Tenemos en E $x \top z = z$, de donde $h(x \top z) = h(z) = \overline{z}$; pero $h(x \top z) = h(x) \overline{\top} h(z) = \overline{x} \overline{\top} \overline{z}$, de donde, al fin, $\overline{x} \overline{\top} \overline{z} = \overline{z}$, $\forall \overline{x} \in \overline{E}$.

3.º Sea $\overline{x} = h(x)$ un elemento cualquiera de $\overline{E}$; la igualdad $e \top x = x$ en E implica, al tomar las imágenes, $h(e \top x) = \overline{e} \overline{\top} \overline{x} = \overline{x}$.

4.º La igualdad $a'' \top a = e$ implica, al tomar las imágenes en $\overline{E}$,

$$h(a'' \top a) = \overline{a''} \overline{\top} \overline{a} = \overline{e}.$$

Dos elementos x, y de E se llaman *permutables* si se tiene

$$x \top y = y \top x.$$

Para esto mismo también se dice que x e y *conmutan*.

Un elemento a permutable con todo elemento de E :

$$a \top x = x \top a \quad \forall x \in E$$

se llama *central*. El conjunto de los elementos centrales es, por definición, el *centro* C de E . Un elemento neutro e , un elemento lícito z , si existen en E , pertenecen al centro C . En otros casos puede acontecer que el centro sea un conjunto vacío. Otro caso extremo por lo contrario, es aquel en que el centro C de E coincide con E : este caso ocurre cuando dos elementos cualesquiera x, y de E conmutan:

$$x \top y = y \top x \quad \forall x, y \in E$$

Se dice entonces que la ley de composición considerada es *conmutativa*, y que E es *conmutativo* o *abeliano*. Si E es finito, la conmutatividad se traduce en el hecho de que la tabla de E sea simétrica con relación a la diagonal principal.

Teorema 2. — Sea $\overline{E}$ una imagen homomorfa de E

$$(h) \quad E \sim \overline{E} = h(E).$$

Si dos elementos x, y de E conmutan, sus imágenes $h(x), h(y)$ en $\overline{E}$ también conmutan.

La igualdad $x \top y = y \top x$ implica en efecto $h(x \top y) = h(y \top x)$ es decir, $h(x) \overline{\top} h(y) = h(y) \overline{\top} h(x)$.

Corolario 1. — Si E es abeliano y $\overline{E}$ es imagen homomorfa de E también $\overline{E}$ es abeliano.

En efecto, dos elementos cualesquiera $\bar{x}, \bar{y}$ de $\overline{E}$ son imágenes de los elementos x, y de E : $\bar{x} = h(x), \bar{y} = h(y)$. Basta, pues, aplicar el teorema 2.

En particular, si E es abeliano, el conjunto cociente $E/\mathcal{R}$ de E por una equivalencia regular es abeliano.

Corolario 2. — En todo homomorfismo

$$(h) \quad E \sim \overline{E} = h(E),$$

la imagen $h(C)$ del centro C de E está contenida en el centro $\bar{C}$ de $\bar{E}$.

Es preciso señalar que no es, en general, $h(C) = \bar{C}$. Veremos más adelante (cap. III, § 2), un ejemplo en el cual la inclusión $h(C) \subset \bar{C}$ es estricta.

Ejemplos. — La adición, la multiplicación de los números naturales, racionales, reales o complejos son conmutativas. La formación del m.c.d. —y la del m.c.m.— en el conjunto $\mathbf{N}$ de los números naturales son leyes de composición conmutativas e idempotentes. La ley de composición $\mathbf{T}$ definida en el conjunto $\mathbf{R}^+$ de los números reales positivos por

$$a \mathbf{T} b = a^b$$

no es conmutativa. De la misma manera, la composición de movimientos (en el plano por ejemplo) no es conmutativa, como hemos visto en el § 1.

Diremos que dos partes A, B de E son *permutables* (o *conmutan*) si se tiene

$$(1) \quad A \mathbf{T} B = B \mathbf{T} A$$

en el sentido del § 4, 4.º. La parte vacía es permutable con toda parte X , ya que es elemento lícito de $\mathcal{P}(E)$. En el caso $A \neq \emptyset, B \neq \emptyset$, la relación (1) significa que cada uno de los miembros está contenido en el otro, puesto que:

$$\forall a \in A, \forall b \in B, \quad \exists a' \in A \text{ y } b' \in B \text{ tales que } ab = b'a'$$

y

$$\forall a \in A, \forall b \in B, \quad \exists a'' \in A \text{ y } b'' \in B \text{ tales que } ba = a''b''.$$

En particular, un elemento x y una parte $A (\neq \emptyset)$ de E son permutables si se tiene

$$(2) \quad x \mathbf{T} A = A \mathbf{T} x.$$

Esta igualdad (que es la que se escribe, en vez de $\{x\} \mathbf{T} A = A \mathbf{T} \{x\}$) significa que:

$$\forall a \in A, \quad \exists a' \in A \text{ tal que } x \mathbf{T} a = a' \mathbf{T} x$$

y

$$\forall a \in A, \quad \exists a'' \in A \text{ tal que } a \mathbf{T} x = x \mathbf{T} a''.$$

Para dos partes de E reducidas cada una a un elemento, se vuelve a encontrar la definición de permutabilidad entre estos elementos.

Un elemento x que vérifica en E la igualdad

$$x \top a = m$$

se llama *complementario a la izquierda* de m por a o (especialmente en notación multiplicativa) *cociente a la izquierda* de m por a .

Si, cualesquiera que sean $a, m \in E$, existe al menos un cociente a la izquierda de m por a , se dice que E verifica la *condición de existencia de cocientes a la izquierda*.

Decir que, cualesquiera que sean $a, m \in E$, existe a lo más un cociente a la izquierda de m por a , equivale a decir que E verifica la regla de simplificación a la derecha. La conjunción de la existencia de los cocientes a la izquierda y de la regla de simplificación a la derecha es, pues, una condición necesaria y suficiente para la existencia y unicidad del cociente a la izquierda: esta condición se designa con la expresión de *axioma de los cocientes a la izquierda*. Cuando se cumple, la ley que asocia al par ordenado (m, a) el cociente a la izquierda x es llamada *ley inversa a la izquierda de la ley $\top$ considerada*.

Se llama *axioma de los cocientes* la conjunción del axioma de los cocientes a la derecha y del axioma de los cocientes a la izquierda.

Teorema 3. — Si E verifica la condición de existencia de cocientes a la izquierda, toda imagen homomorfa $\overline{E} = h(E)$ la verifica también.

Sean en efecto, $\overline{a}, \overline{m}$ dos elementos cualesquiera de $\overline{E}$; y a, m dos elementos de E que los tienen respectivamente por imágenes. Por hipótesis, existe en E al menos un elemento x tal que

$$x \top a = m$$

de donde, pasando a las imágenes:

$$h(x) \overline{\top} h(a) = h(m)$$

el elemento $\overline{x} = h(x)$ de $\overline{E}$ es pues cociente a la izquierda de $\overline{m} = h(m)$ por $\overline{a} = h(a)$.

Un teorema análogo es válido, naturalmente, para los cocientes a la derecha.

§ 8. Partes notables de un conjunto E con una ley de composición interna

Recordemos que una parte (o subconjunto) estable del conjunto E con la ley de composición T es una parte S de E tal, que las relaciones $s_1 \in S, s_2 \in S, s_1 T s_2 \notin S$ no pueden verificarse simultáneamente. La parte vacía pertenece a la familia $\mathcal{S}$ de las partes estables.

Teorema 1. — *La familia $\mathcal{S}$ de las partes estables de E es una familia de Moore.*

Está claro, en efecto, que E pertenece a $\mathcal{S}$ y que toda intersección de partes estables es una parte estable.

A la familia de Moore $\mathcal{S}$ viene asociada una clausura de Moore

$$X \rightarrow \bar{X} = X_{\mathcal{S}}$$

donde por definición (§ 4, 5º), $X_{\mathcal{S}}$ es la menor parte estable que contiene a X (subconjunto cualquiera de E). Se dice $X_{\mathcal{S}}$ es la parte estable de E engendrada por X .

Sea h un homomorfismo que aplica E en E' , con la ley de composición T' .

Teorema 2. — a) *La imagen homomorfa $h(S)$ de una parte estable S de E es una parte estable de E' .*

b) *La imagen recíproca $h^{-1}(S')$ de una parte estable S' de E' es una parte estable de E .*

a) Si $s'_1, s'_2 \in S'$, tenemos $s'_i = h(s_i)$ donde $s_i \in S$ ($i = 1, 2$) y por consiguiente

$$h(s_1 T s_2) = [h(s_1)] T' [h(s_2)] = s'_1 T' s'_2.$$

Pero $s_1 T s_2 \in S$, luego $s'_1 T' s'_2 \in S'$.

b) Si $s_1, s_2 \in h^{-1}(S')$, es decir $h(s_i) \in S'$, tenemos

$$h(s_1 T s_2) = [h(s_1)] T' [h(s_2)] \in S'$$

ya que S' es estable; por consiguiente $s_1 T s_2 \in h^{-1}(S')$.

Caso particular. — Si e' es un elemento idempotente de E' , su imagen recíproca $h^{-1}(e')$ es un subconjunto estable de E (vacío si $e' \notin \bar{E} = h(E)$).

Se dice que un subconjunto D de E es *lícito a la derecha* si se tiene

$$D \cap E \subseteq D$$

es decir

$$a \in D \quad \text{implica} \quad a \cap x \in D, \quad \forall x \in E.$$

(o, lo que es lo mismo, si las relaciones $a \in D$, $x \in E$, $a \cap x \notin D$ no pueden verificarse simultáneamente). El subconjunto vacío $\emptyset$, pertenece a la familia $\mathfrak{D}$ de los subconjuntos o partes lícitas a la derecha.

Cualquier subconjunto lícito a la derecha, D , es estable, puesto que se tiene

$$D \cap D \subseteq D \cap E \subseteq D.$$

Se define de forma simétrica un subconjunto *lícito a la izquierda* G :

$$E \cap G \subseteq G$$

y se llama *parte lícita* a una parte P , que sea a la vez, lícita por la derecha y por la izquierda. Sea $\mathfrak{G}$ la familia de las partes lícitas a la izquierda, y $\mathfrak{F}$ la familia de las partes lícitas; se tiene

$$\mathfrak{F} = \mathfrak{G} \cap \mathfrak{D}$$

Ejemplos. — El subconjunto $\{z\}$ constituido por un elemento lícito a la izquierda es lícito a la izquierda. En el conjunto $\mathbf{N}$ de los números naturales, con la multiplicación, el conjunto $\mathbf{P}$ de los números pares es una parte lícita.

Teorema 3. — La familia $\mathfrak{D}$ de las partes de E lícitas a la derecha es una familia de Moore, así como las familias $\mathfrak{G}$ y $\mathfrak{F}$.

Es obvio que E pertenece a $\mathfrak{D}$ y que toda intersección de subconjuntos lícitos a la derecha es lícita a la derecha. El mismo razonamiento para $\mathfrak{G}$. Y se sabe, finalmente, que la intersección de familias de Moore es también una familia de Moore.

Se advierten las inclusiones

$$\mathfrak{F} \subseteq \mathfrak{D} \subseteq \mathfrak{S}, \quad \mathfrak{F} \subseteq \mathfrak{G} \subseteq \mathfrak{S}.$$

A las familias de Moore $\mathfrak{D}$, $\mathfrak{G}$, $\mathfrak{F}$ están asociadas las clausuras de Moore:

$$X \rightarrow X_{\mathfrak{D}}, \quad X \rightarrow X_{\mathfrak{G}}, \quad X \rightarrow X_{\mathfrak{F}}.$$

Por definición $X_{\mathfrak{D}}$, $X_{\mathfrak{G}}$, $X_{\mathfrak{T}}$ son, respectivamente, la mínima parte lícita en E que contienen a X , o engendradas por X .

Teorema 4. — Sea h un homomorfismo que aplica E con la ley $\mathfrak{T}$, sobre $\overline{E}$ con la ley $\overline{\mathfrak{T}}$:

$$(h) \quad E \sim \overline{E} = h(E).$$

La imagen $\overline{D}$ de una parte lícita a la derecha, D , de E es, en $\overline{E}$, una parte lícita a la derecha.

El teorema es evidente cuando D es vacío.

Sean, pues, $\overline{a} \in h(D)$, $\overline{x} \in \overline{E}$; existe al menos un elemento a de D y al menos un elemento x de E tales que

$$h(a) = \overline{a}, \quad h(x) = \overline{x}.$$

Tenemos $a \mathfrak{T} x \in D$, de donde $h(a \mathfrak{T} x) \in h(D)$.

Ahora, $h(a \mathfrak{T} x) = h(a) \overline{\mathfrak{T}} h(x) = \overline{a} \overline{\mathfrak{T}} \overline{x}$ y $\overline{a} \overline{\mathfrak{T}} \overline{x} \in \overline{D}$.

Observación. — Para un homomorfismo h de E en E' , el teorema precedente no conserva su validez en general. Tomemos por ejemplo para E el conjunto $\mathbf{N} = \{1, 2, \dots, n, \dots\}$ de los enteros naturales con la multiplicación, para D el conjunto de los números naturales pares, $D = \{2, 4, \dots\}$ para E' el conjunto $\mathbf{Z}$ de los enteros de cualquier signo; para h la aplicación idéntica (de $\mathbf{N}$ sobre $\mathbf{N} \subset E'$); con esto, $h(D) = D$ no es una parte lícita de $\mathbf{Z}$ ($2 \in D$, $-1 \in \mathbf{Z}$, $-2 \notin D$).

Para los subconjuntos lícitos a la izquierda y los subconjuntos lícitos son válidas las proposiciones análogas al teorema 4.

Teorema 5. — Sea h un homomorfismo que aplica E en E' :

$$(h) \quad E \rightarrow E'.$$

La imagen recíproca de una parte lícita a la derecha D' de E' es, en E , una parte lícita a la derecha.

El teorema es evidente cuando $h^{-1}(D')$ es vacío.

Sean, pues, $a \in h^{-1}(D')$, $x \in E$. Tenemos:

$$h(a \mathfrak{T} x) = h(a) \mathfrak{T}' h(x)$$

con $h(a) \in D'$, $h(x) \in E'$, de donde $h(a) \top h(x) \in D'$ y por consiguiente

$$a \top x \in h^{-1}(D').$$

Se ve en particular, que la imagen inversa de un elemento z' lícito a la derecha en E' es, en E , una parte lícita a la derecha.

Se dice que una parte U_d de E es *unitaria a la derecha* si

$$u_1 \in U_d, u_2 \in U_d \text{ y } x \top u_1 = u_2 \text{ donde } x \in E \text{ implica } x \in U_d,$$

(o, lo que es lo mismo, si las relaciones $u_1 \in U_d, u_2 \in U_d, x \in \bigcap_E U_d, x \top u_1 = u_2$ no pueden verificarse simultáneamente).

La parte vacía, $\emptyset$, pertenece a la familia $\mathcal{U}_d$ de partes unitarias a la derecha.

Se define de una manera simétrica una *parte unitaria a la izquierda* U_g ($u_1 \in U_g, u_2 \in U_g, u_1 \top x = u_2$, con $x \in E$, implican $x \in U_g$); se llama *parte unitaria* (o *subconjunto unitario*) a una parte U que sea unitaria a la derecha y a la izquierda simultáneamente.

Observación. — Si E con la ley $\top$ verifica el axioma de los cocientes a la izquierda las partes unitarias a la derecha no son otra cosa que las partes estables para la ley inversa a la izquierda de $\top$.

Ejemplo. — Si u es un elemento neutro a la derecha en E , el subconjunto $\{u\}$ constituido por este elemento es unitario a la derecha.

Teorema 6. — La familia $\mathcal{U}_d$ de las partes unitarias a la derecha de un conjunto E con una ley de composición interna es una familia de Moore; la familia $\mathcal{U}_g$ de las partes unitarias a la izquierda y la familia $\mathcal{U}$ de las partes unitarias son también familias de Moore.

Es claro que E pertenece a $\mathcal{U}_d$ y que toda intersección de partes unitarias a la derecha es unitaria a la derecha. El mismo razonamiento vale para $\mathcal{U}_g$ y $\mathcal{U}$; se puede señalar también que $\mathcal{U} = \mathcal{U}_g \cap \mathcal{U}_d$.

A las familias de Moore $\mathcal{U}_g, \mathcal{U}_d, \mathcal{U}$ vienen asociadas las clausuras de Moore

$$X \rightarrow X_{\mathcal{U}_d}, \quad X \rightarrow X_{\mathcal{U}_g}, \quad X \rightarrow X_{\mathcal{U}}$$

donde $X_{\mathcal{U}_d}, X_{\mathcal{U}_g}, X_{\mathcal{U}}$ son respectivamente, el menor subconjunto unitario a la derecha, el menor subconjunto unitario a la izquierda y el menor subconjunto unitario que contienen a X o, como se dice generalmente, engendrados por X .

En el estudio del comportamiento de los subconjuntos unitarios en los homomorfismos, nos limitaremos a los dos teoremas siguientes.

Teorema 7. — *Sea h un homomorfismo que aplica E con cocientes a la izquierda en E' .*

Si U'_a es, en E' , una parte unitaria a la derecha, su imagen recíproca $h^{-1}(U'_a)$ es, en E , una parte unitaria a la derecha U_a .

Sean $u_1, u_2 \in h^{-1}(U'_a)$ y x un cociente a la izquierda de u_2 por u_1 del que suponemos la existencia.

$$x \top u_1 = u_2.$$

Tenemos

$$h(x) \top' h(u_1) = h(u_2), \quad \text{donde } h(u_i) \in U'_a \quad (i = 1, 2)$$

de donde, por ser U'_a unitario a la derecha,

$$h(x) \in U'_a \quad \text{y} \quad x \in h^{-1}(U'_a) = U_a.$$

Resulta, en particular, que la imagen recíproca $h^{-1}(e')$ de un elemento e' neutro a la derecha en E' es, en E , una parte unitaria a la derecha.

Mientras que el teorema precedente, relativo a la *imagen inversa*, es válido para conjuntos E con cocientes a la izquierda, E' cualesquiera, en cambio, para establecer que la imagen homomorfa de una parte unitaria es una parte unitaria, se deben hacer hipótesis bastante fuertes sobre E y E' . Demostraremos la siguiente proposición:

Teorema 8. — *Sea h un homomorfismo de E en E'*

$$(h) \quad E \rightarrow E'.$$

Si E verifica la condición de existencia de cocientes a la izquierda y E' la regla de simplificación a la derecha, la imagen $h(U_a)$ de una parte unitaria a la derecha U_a de E es una parte unitaria a la derecha de E' .

Sean $u'_1, u'_2 \in h(U_a)$ e y' un elemento de E' , que cumplen la relación

$$y' \top' u'_1 = u'_2$$

Consideremos dos elementos u_1, u_2 de U_a que tengan respectivamente u'_1, u'_2 por imágenes; por hipótesis existirá al menos un cociente a la izquierda de u'_2 por u'_1 :

$$x \top u_1 = u_2.$$

y este cociente x pertenece a U_d puesto que U_d es unitario a la derecha.
Tomando las imágenes de los dos miembros obtendremos

$$h(x) \top' u'_1 = u'_2 = y' \top' u'_1$$

de donde, puesto que E' verifica la regla de simplificación a la derecha

$$y' \in h(U_d)$$

como queríamos demostrar.

CAPÍTULO II

SEMIGRUPOS. GRUPOS

§ 1. Asociatividad. Semigrupos

En un conjunto E con la ley de composición T ocurre a veces, que después de componer dos elementos, el resultado deba componerse con un tercero, etc..., o bien, deben componerse entre sí los resultados de componer dos pares de elementos, etc... Los paréntesis, corchetes, ..., permiten simbolizar cómodamente esta sucesión de operaciones. Si se forma por ejemplo $a T b = r$, y luego $r T c = x$, se escribirá $x = (a T b) T c$; si se forma $b T c = s$ y luego $a T s = y$, se escribirá $y = a T (b T c)$. Lo mismo $(a T b) T (c T d)$ indica $u T v$, donde $u = a T b$ y $v = c T d$, mientras que $[(a T b) T c] T d$ indica $m T d$, donde $m = n T c$ y $n = a T b$.

Tomando n elementos ($n > 2$) en un orden fijado, existen, como acabamos de ver, diversas maneras de componerlos sucesivamente, y no hay ninguna razón para que los resultados obtenidos sean iguales entre sí. Por ejemplo, si T designa la formación de la media aritmética en el conjunto de los números reales, $a T b = (a + b)/2$, se tiene

$$(a T b) T c = \frac{a + b + 2c}{4}, \quad a T (b T c) = \frac{2a + b + c}{4}$$

y estos dos números son en general diferentes.

Lo mismo, si $\wedge$ designa la formación del producto vectorial (en el espacio de tres dimensiones), los vectores $(\vec{a} \wedge \vec{b}) \wedge \vec{c}$ y $\vec{a} \wedge (\vec{b} \wedge \vec{c})$, son en general distintos. En el conjunto E con la ley de composición interna definida por la tabla

T	a	b	c
a	b	c	a
b	b	c	a
c	b	c	a

se tiene

$$\begin{aligned}(a \top a) \top a &= b \top a = b, & a \top (a \top a) &= a \top b = c \\ [(a \top a) \top a] \top a &= b \top a = b, & (a \top a) \top (a \top a) &= b \top b = c, \\ a \top [a \top (a \top a)] &= a \top c = a.\end{aligned}$$

Sin embargo, sabemos que en muchos casos, por ejemplo en la adición o multiplicación de los números naturales, racionales, reales o complejos, no existen estas complicaciones, y esto se debe a que la correspondiente ley de composición es una ley *asociativa*.

Se dice que la ley de composición $\top$ de D es *asociativa* si se tiene

$$(1) \quad (x \top y) \top z = x \top (y \top z) \quad \forall x, y, z \in D;$$

En este caso D se llama *semigrupo*¹ (o también *monoide*). Generalmente se emplea la *notación multiplicativa* para la ley de composición de un semigrupo D ; con esta notación, (1) se escribe

$$(1') \quad (xy)z = x(yz) \quad \forall x, y, z \in D$$

Es cómodo representar el valor común de los dos miembros por el *símbolo único* xyz ; xyz es lo que se llama el *producto de los tres elementos* x, y, z tomados en este orden.

Más generalmente, consideremos, en un semigrupo multiplicativo D , n elementos $a_1, a_2, \dots, a_n$ (distintos o no) ordenados según los índices crecientes. Escribamos:

$$p = \{ \dots [(a_1 a_2) a_3] a_4 \dots \} a_n.$$

Teorema 1. — *Cualquier otro producto p' formado con los factores $a_1, \dots, a_n$, tomados en este orden es igual a p .*

Según (1'), la proposición es cierta para $n = 3$. Supongamos que se cumple para m factores, cualquiera sea $m < n$.

El producto p' es de la forma

$$p' = p'_1 p'_2,$$

donde p'_1 está formado con $a_1, \dots, a_h$, p'_2 con $a_{h+1}, \dots, a_n$ ($1 \leq h \leq n - 1$).

Si $h = n - 1$, se tiene $p'_2 = a_n$, p'_1 será entonces un producto formado con los $n - 1$ factores $a_1, \dots, a_{n-1}$ y según la hipótesis de recurrencia,

$$p'_1 = a_1 \dots a_{n-1},$$

de donde $p' = p$.

¹ “*Demi-groupe* (ou *semi-groupe*)” en el original, donde se advierte: También se ha utilizado la locución “*semi-groupe*” para designar a D en el caso de ser válida la regla de simplificación, además de la asociativa, pero aquí no adoptaremos esta terminología.

En los otros casos se tiene, siempre por la hipótesis de recurrencia:

$$p'_1 = a_1 \dots a_h, \quad p'_2 = a_{h+1} \dots a_n, \quad \text{con} \quad 1 \leq h \leq n-2,$$

luego

$$p' = (a_1 \dots a_h) \cdot (a_{h+1} \dots a_n) = (a_1 \dots a_h) [(a_{h+1} \dots a_{n-1})a_n] \quad /$$

de donde, según (1')

$$p' = [(a_1 \dots a_h) (a_{h+1} \dots a_{n-1})] a_n$$

y, según la hipótesis de recurrencia,

$$p' = (a_1 \dots a_{n-1})a_n = p.$$

Corolario. — En un semigrupo se puede hablar de la *potencia m-ésima de un elemento a*, producto de *m* elementos *a*, que puede efectuarse componiendo los elementos de cualquier manera. Se designa este elemento por a^m y se tiene la regla:

$$a^m a^n = a^{m+n}$$

Teorema 2. — En un semigrupo abeliano, el producto

$$p = a_1 a_2 \dots a_n$$

es independiente del orden de los factores.

Si primeramente permutamos dos factores consecutivos, tenemos

$$a_1 \dots a_i a_{i+1} \dots a_n = a_1 \dots a_{i+1} a_i \dots a_n.$$

En efecto, pongamos (para $i \neq 1, n-1$)

$$a_1 \dots a_{i-1} = r, \quad a_i a_{i+1} = s = a_{i+1} a_i, \quad t = a_{i+2} \dots a_n;$$

y los dos miembros de la igualdad a establecer coinciden, efectivamente, con el producto $r s t$. El razonamiento es análogo (con simplificación de escritura) si $i = 1$ ó $i = n-1$.

Para obtener la proposición general bastará ya fijarse en que se pasa de la permutación $a_1 a_2 \dots a_n$ a otra permutación cualquiera con una serie de transposiciones entre elementos consecutivos. Este hecho es evidente para $n = 2$, y se generaliza por recurrencia sobre n : se puede, por cambios de elementos consecutivos, llevar, si es necesario, al primer lugar el elemento a que debe encon-

trarse allí, y para el producto de los $n - 1$ factores restantes, la posibilidad enunciada existe por la hipótesis de recurrencia.

Demos algunos ejemplos de semigrupos o de leyes asociativas.

Ejemplo 1. — La *intersección* $\cap$ y la *unión* $\cup$ de *partes* de un conjunto E son leyes de composición *asociativas* (y además, conmutativas e idempotentes).

Ejemplo 2. — El conjunto de los números naturales $\mathbf{N} = \{ 1, 2, \dots, n \}$, con una cualquiera de las leyes de composición siguientes:

adición,
multiplicación,
formación del m.c.d.
formación del m.c.m.

es un semigrupo abeliano. El conjunto $\mathbf{Z}$ de los enteros de signo cualquiera es un semigrupo abeliano aditivo, y un semigrupo abeliano multiplicativo.

Ejemplo 3. — El conjunto de los números racionales positivos $\mathbf{Q}^+$ es un semigrupo multiplicativo; lo mismo para el conjunto $\mathbf{Q}$ de todos los racionales, el conjunto $\mathbf{R}^+$ de los números reales positivos, el conjunto $\mathbf{R}$ de todos los números reales y el conjunto $\mathbf{C}$ de los números complejos. Todos estos semigrupos son abelianos.

Ejemplo 4. — La *composición* $\circ$ de las *aplicaciones* de un conjunto E en sí mismo es *asociativa*: $(\alpha \circ \beta) \circ \gamma$ y $\alpha \circ (\beta \circ \gamma)$ son, una y otra, la aplicación $\tilde{\omega}$ consistente en efectuar sucesivamente (y en este orden) γ, β, α :

$$\tilde{\omega}x = \alpha \{ \beta[\gamma(x)] \} \quad \forall x \in E.$$

Estas aplicaciones forman pues un semigrupo $\mathcal{A}$ (obsérvese que si E posee más de un elemento, $\mathcal{A}$ no es abeliano).

Si α y β son dos aplicaciones *inyectivas*, o *exhaustivas*, o *biyectivas*, la aplicación compuesta $\alpha \circ \beta$ tiene la propiedad correspondiente. El conjunto $\mathcal{I}$ de aplicaciones inyectivas, el conjunto $\mathcal{S}$ de aplicaciones exhaustivas, el conjunto $\mathcal{B}$ de aplicaciones biyectivas de E en o sobre sí mismo son pues semigrupos, contenidos en $\mathcal{A}$. Las aplicaciones biyectivas se llaman también *transformaciones* de E . Si E es un conjunto *finito*, se tiene $\mathcal{I} = \mathcal{S} = \mathcal{B}$ (si todo elemento se obtiene a lo más una vez, o al menos una vez como imagen, se obtiene exactamente una vez); en este caso las transformaciones de E se llaman *permutaciones* (o *sustituciones*).

Se han visto en el capítulo primero (§ 4) varios procedimientos fundamentales

para construir a partir de conjuntos dados con leyes de composición interna, un nuevo conjunto con ley de composición interna. Si los conjuntos dados son semigrupos, el resultado de la construcción en varios de los casos examinados también lo es.

1.º Es claro, en primer lugar, que el conjunto $\mathcal{F}$ de las funciones definidas sobre un conjunto X y que toman sus valores en un semigrupo D , es otro semigrupo, con la ley de composición definida en el capítulo primero.

2.º El producto de semigrupos $D_1, D_2, \dots, D_k$ es igualmente un semigrupo.

3.º Una parte estable S de un semigrupo D será denominada *subsemigrupo*, puesto que la restricción a S de la ley asociativa de D es evidentemente una ley asociativa en S . Así, el conjunto de los números naturales $\mathbf{N}$, con la suma o con la multiplicación, admite como subsemigrupo el conjunto de los enteros pares. El semigrupo $\mathcal{A}$ de las aplicaciones de un conjunto E en sí mismo contiene como subsemigrupo los conjuntos $\mathcal{I}$ y $\mathcal{S}$ de las aplicaciones inyectivas y de las aplicaciones exhaustivas; cada una de éstas contiene como subsemigrupo el conjunto $\mathcal{B}(=\mathcal{I} \cap \mathcal{S})$ de las transformaciones biyectivas.

4.º Por extensión al conjunto de las partes, $\mathcal{P}(D)$, la ley de composición de un semigrupo D define una ley asociativa:

$$(2) \quad (AB)C = A(BC) \quad \forall A, B, C \in \mathcal{P}(D).$$

En efecto, si A, B, C no son vacías, se tiene

$$\begin{aligned} (AB)C &= \{ (ab)c ; a \in A, b \in B, c \in C \} \\ A(BC) &= \{ a(bc) ; a \in A, b \in B, c \in C \} \end{aligned}$$

y, puesto que $(ab)c = a(bc)$, estos dos conjuntos coinciden. Si una al menos de las partes A, B, C es vacía, los dos miembros de (2) resultan iguales a la parte vacía. $\mathcal{P}(D)$ es, pues, un semigrupo, al que se llama *semigrupo de las partes*. Cuando D sea abeliano, también lo será.

5.º La ley $\bar{\mathbf{T}}$ definida en una familia de Moore $\mathcal{F} \subseteq \mathcal{P}(E)$ a partir de una ley $\mathbf{T}$ asociativa dada en E (ver Cap. I, § 4, 5.º) no es en general asociativa, como muestra el ejemplo siguiente.

Consideremos el conjunto E de los números 1, 2, 3, 4, 6, y como ley de composición $\mathbf{T}$, la formación del m.c.d.:

$$x \mathbf{T} y = \text{m.c.d. } (x, y).$$

Esta ley $\mathbf{T}$ es asociativa y conmutativa (y también idempotente): E es un semigrupo abeliano.

En $\mathcal{P}(E)$, la familia $\mathcal{F}$ formada por $E, A = \{6\}, B = \{4\}, C = \{3\}$,

$D = \{1\}$ y $\emptyset$ es una familia de Moore. Mostremos que en $\mathcal{F}$ la ley de composición $\bar{\tau}$ (definida como se ha visto en el Cap. I, § 4, 5.º) no es asociativa.

Tenemos $\{6\} \tau \{4\} = \{2\}$ de donde $A \bar{\tau} B = \overline{\{2\}} = E$, además

$$E \tau C = \{1, 3\} \quad \text{luego} \quad E \bar{\tau} C = \overline{\{1, 3\}} = E,$$

luego

$$(A \bar{\tau} B) \bar{\tau} C = E.$$

Por otra parte, $\{4\} \tau \{3\} = \{1\}$ luego $B \tau C = D = B \bar{\tau} C$,

y

$$\{6\} \tau \{1\} = \{1\} \quad \text{luego} \quad A \bar{\tau} D = \overline{\{1\}} = \{1\} = D,$$

de donde

$$A \bar{\tau} (B \bar{\tau} C) = D \neq E.$$

6.º Sea D un semigrupo y $\bar{D} = h(D)$ la imagen homomorfa de D en un homomorfismo h :

$$(h) \quad D \sim \bar{D} = h(D).$$

Dados tres elementos cualesquiera (distintos o no) $\bar{x}, \bar{y}, \bar{z}$ de $\bar{D}$ existen en D elementos x, y, z que los tienen por imágenes respectivas. La igualdad $(xy)z = x(yz)$ implica, tomando las imágenes,

$$(\bar{x}\bar{y})\bar{z} = \bar{x}(\bar{y}\bar{z}).$$

Como esta última igualdad resulta cierta cualesquiera sean $\bar{x}, \bar{y}, \bar{z} \in \bar{D}$, $\bar{D}$ es un semigrupo. Así:

Teorema 3. — *Toda imagen homomorfa de un semigrupo es un semigrupo.*

En particular, el conjunto cociente $D/\mathcal{R}$ de un semigrupo D por una relación de equivalencia regular $\mathcal{R}$ es un semigrupo, llamado semigrupo cociente.

Por ejemplo, el conjunto $\mathbf{Z}/(n)$ de las clases residuales módulo n es a la vez un semigrupo abeliano aditivo y un semigrupo abeliano multiplicativo.

La asociatividad de una ley de composición implica todavía numerosas propiedades, tales como las siguientes.

Teorema 4. — *En un semigrupo D , el centro Z es una parte estable (eventualmente vacía)*

Si $z_1, z_2 \in Z$, se tiene, cualquiera sea $x \in D$:

$$(z_1 z_2)x = z_1(z_2 x) = z_1(x z_2) = (z_1 x)z_2 = (x z_1)z_2 = x(z_1 z_2)$$

luego $z_1 z_2 \in Z$.

Teorema 5. — *En un semigrupo D , el producto LR de una parte lícita a la izquierda L por una parte lícita a la derecha R es una parte lícita.*

Se tiene en efecto

$$D(LR) = (DL)R \subseteq LR,$$

$$(LR)D = L(RD) \subseteq LR.$$

Observación. — Indiquemos por $\mathcal{A}$ el conjunto de partes de D lícitas a la izquierda, $\mathcal{L}$, por $\mathcal{B}$ el conjunto de partes lícitas a la derecha, $\mathcal{R}$, por $\mathcal{C}$ el conjunto de partes lícitas: el teorema precedente ofrece un nuevo ejemplo de ley de composición en el sentido más general de aplicación del conjunto producto $\mathcal{A} \times \mathcal{B}$ en $\mathcal{C}$ (cfr. Cap. I, § 2).

Teorema 6. — *En un semigrupo D , el conjunto T de los elementos t simplificables a la izquierda es un subsemigrupo unitario a la izquierda.*

Sean $t_1, t_2 \in T$. Si

$$(t_1 t_2)x = (t_1 t_2)y,$$

se puede escribir

$$t_1(t_2 x) = t_1(t_2 y),$$

de donde

$$t_2 x = t_2 y,$$

es decir

$$x = y.$$

Se tiene, pues, $t_1 t_2 \in T$ y T es efectivamente un subsemigrupo (en el cual, evidentemente, vale la regla de simplificación a la izquierda).

Sea ahora $tr = t'$, con $t, t' \in T$. La igualdad

$$rx = ry$$

implica

$$t(rx) = t(ry) \quad \text{o} \quad (tr)x = (tr)y,$$

es decir,

$$t'x = t'y, \quad \text{luego} \quad x = y.$$

Por consiguiente, $r \in T$ y T es efectivamente unitario a la izquierda.

Observación. — Es válido el teorema de enunciado simétrico. El conjunto de elementos simplificables constituye pues, un subsemigrupo, pero no se puede afirmar que sea unitario; en efecto, si t y t' son simplificables y $tr = t'$, sólo se puede concluir que r es simplificable a la izquierda.

Teorema 7. — *En un semigrupo D con elemento unidad a la derecha e , todo elemento con inverso a la derecha es simplificable a la derecha.*

Sea a un elemento; por hipótesis existirá un elemento a' tal que $aa' = e$. La igualdad

$$xa = ya$$

implica

$$(xa)a' = (ya)a' \quad \text{luego} \quad x(aa') = y(aa')$$

es decir $xe = ye$ o en fin $x = y$.

Corolario. — *En un semigrupo D con elemento unidad e , todo elemento simetrizable es simplificable (o regular).*

Teorema 8. — *Si un semigrupo D tiene un elemento neutro por un lado al menos e , el conjunto Δ de los elementos de D con inverso a la derecha respecto a e , es un subsemigrupo de D .*

Sean $a, b \in \Delta$ y, por tanto, $aa' = e = bb'$. Tendremos:

$$(ab)(b'a') = a(bb')a' = aea' = aa' = e$$

puesto que, si e es neutro a la derecha, $aea' = (ae)a' = aa'$ y, si e es neutro a la izquierda, $aea' = a(ea') = aa'$.

Teorema 9. — *En un semigrupo D con un elemento unidad bilátera e , si un elemento a tiene (con relación a e) un inverso a la derecha a' y un inverso a la izquierda a'' , debe ser $a' = a''$: en un semigrupo de este tipo todo elemento con inverso es simetrizable y tiene un solo inverso.*

Tenemos por hipótesis $aa' = e = a''a$, de donde

$$(a''a)a' = ea' = a' \quad a''(aa') = a''e = a''$$

y en consecuencia $a' = a''$, ya que $(a''a)a' = a''(aa')$.

Según lo anterior, a no admite otro inverso que $a' = a''$; como ya se ha dicho, este inverso único se indica en notación multiplicativa por a^{-1} .

Teorema 10. — Si en un semigrupo multiplicativo D , un elemento e verifica una relación de la forma

$$es = s$$

siendo s un elemento simplificable a la derecha, e es neutro a la derecha.

En efecto, se tiene para todo elemento x de D ,

$$(xe)s = x(es) = xs$$

de donde

$$xe = x \quad (\forall x \in D).$$

Corolario 1. — En un semigrupo D que verifica la regla de simplificación a la derecha, todo elemento idempotente s es unidad a la derecha.

Corolario 2. — Un semigrupo en el que valga la regla de simplificación tiene a lo sumo un elemento idempotente que, si existe, es elemento unidad.

En un semigrupo se puede considerar la familia $\mathcal{R}$ de las partes semiprimas (o aisladas) R , caracterizadas por la propiedad de que si alguna potencia de un elemento d pertenece a R , también d pertenece a R (dicho de otro modo: las relaciones $d^n \in R$, y $d \notin R$ son incompatibles).

Teorema 11. — En un semigrupo multiplicativo D , las partes semiprimas R forman una familia de Moore $\mathcal{R}$.

En efecto, es evidente que D es semiprimo, así como toda intersección de partes semiprimas.

A la familia de Moore $\mathcal{R}$ viene asociada una clausura de Moore en $\mathcal{P}(D) : X \rightarrow \bar{X} = X_{\mathcal{R}}$. Por definición $X_{\mathcal{R}}$ es la menor parte semiprima que contiene a X . Se dice que $X_{\mathcal{R}}$ es la parte semiprima engendrada por X : y también que $X_{\mathcal{R}}$ es el radical de X .

El radical $X_{\mathcal{R}}$ de X coincide con el conjunto de los elementos del semigrupo D para los que alguna potencia pertenece a X . En efecto sea Y este conjunto; $y \in Y$, quiere decir $y^n \in X \subseteq X_{\mathcal{R}}$ para algún n ($= 1, 2, \dots$), lo que implica $y \in X_{\mathcal{R}}$; tenemos pues $Y \subseteq X_{\mathcal{R}}$. Por otra parte, Y contiene a X y es parte semiprima, pues $z^m \in Y$, es decir $z^{mm'} \in X$ implica $z \in Y$; resulta $X_{\mathcal{R}} \subseteq Y$, y debe, pues, valer la igualdad.

§ 2. Grupos. Axiomática de grupo

Un grupo G es un conjunto con una ley de composición interna, para la

que aquí adoptaremos notación multiplicativa, que cumple las *condiciones siguientes*:

$$\Sigma \left\{ \begin{array}{l} \text{I, } G \text{ es un semigrupo, es decir, su ley de composición es asociativa} \\ \quad ((xy)z = x(yz) \quad \forall x, y, z \in G); \\ \text{II, Existe en } G \text{ un elemento neutro } e (ex = xe = x, \forall x \in G); \\ \text{III, Todo elemento } x \text{ de } G \text{ tiene un simétrico respecto a } e (\forall x \in G, \text{ existe} \\ \quad \text{en } G \text{ un elemento } x^* \text{ tal que } xx^* = x^*x = e). \end{array} \right.$$

De estas tres propiedades resultan inmediatamente algunas consecuencias importantes.

G no es vacío, puesto que $G \ni e$.

Del corolario del teorema 7, § 1, se deduce que todo elemento de G , por tener simétrico, es regular o simplificable, luego:

IV, En un grupo G se cumple la ley de simplificación.

Resulta con esto que el simétrico x^* de cada elemento x de G es *único*; le llamaremos pues, en la notación multiplicativa, el inverso de x y lo designaremos por x^{-1} .

Consideremos dos elementos a, m de G , e intentemos resolver en G la ecuación

$$(1) \quad ax = m.$$

Multiplicando a la izquierda por a^{-1} , obtenemos

$$x = a^{-1}m$$

y el problema tiene a lo sumo esta solución; que sí lo es, en efecto, puesto que

$$a(a^{-1}m) = (aa^{-1})m = em = m.$$

Así, en un grupo G la ecuación (1) admite la solución única $x = a^{-1}m$, es decir, existe siempre el cociente a la derecha de m por a ; existe análogamente un solo cociente a la izquierda de m por a , $y = ma^{-1}$, solución de la ecuación

$$(1') \quad ya = m.$$

Por esto enunciaremos: en todo grupo G se cumple el axioma de los cocientes, es decir:

$\forall, \forall a, m \in G$, existe un único cociente a la derecha y un único cociente a la izquierda de m por a .

Un grupo G cuya ley de composición es conmutativa se llama *abeliano*. Para los grupos abelianos se utiliza frecuentemente la *notación aditiva*.¹

Además de las reglas de cálculo de los semigrupos, se tiene en un grupo la regla fundamental para la inversión

$$(ab)^{-1} = b^{-1}a^{-1}$$

puesto que (como se ha visto además en § 1, teor. 8)

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

Esta regla se extiende inmediatamente al producto de un número n cualquiera de factores. Se tiene en particular

$$(a^n)^{-1} = (a^{-1})^n$$

para todo entero positivo n ; se ha convenido en escribir más simplemente este elemento, en la forma a^{-n} ; poniendo además $a^0 = e$, tendremos definido a^λ para todo entero λ (los elementos a^λ así obtenidos no tienen por que ser distintos entre sí). Se tiene

$$a^\lambda a^\mu = a^{\lambda+\mu} \quad \forall \lambda, \mu \in \mathbb{Z}.$$

Solamente cuando el grupo G es abeliano se cumple la igualdad $(ab)^\lambda = a^\lambda b^\lambda$; con la notación aditiva a^λ se reemplaza por λa , y la fórmula anterior se escribe $\lambda(a + b) = \lambda a + \lambda b$.

Se llama *orden* de un grupo *finito* G el número N , ó $N(G)$, de sus elementos. frecuentemente designado, también, por $O(G)$.

En la definición de un grupo, el sistema Σ de axiomas, I (asociativo), II (elemento neutro e), III (existencia de inverso respecto a e), puede ser reemplazado por un sistema *equivalente*, pero en el cual cada uno de los axiomas II y III aparece, *individualmente*, debilitado:

¹ *Notación aditiva.* — El elemento neutro se indica por 0, el inverso de a se suele llamar opuesto, y se representa por $-a$; para lo que sigue, en vez de la notación de potencias: $a \cdot a \cdot \dots \cdot a = a^m$ se utiliza la de múltiplos naturales: $a + a + \dots + a = ma$; $-ma = m(-a)$; finalmente, $0a = 0$ (el primer 0 es el número cero, el segundo es el elemento neutro del grupo *aditivo*). (N. del T.)

$$\Sigma' \left\{ \begin{array}{l} \text{I, asociatividad de la ley de composición;} \\ \text{II', existe en el conjunto } D \text{ considerado, al menos un elemento neutro a} \\ \text{la derecha, } e: \\ \text{III', con relación a } e, \text{ todo elemento } x \text{ de } D \text{ admite al menos un inverso} \\ \text{a la derecha } x' : xx' = e. \end{array} \right.$$

Es evidente que Σ implica Σ' . Para obtener el recíproco estableceremos el teorema siguiente, para un *semigrupo multiplicativo* D que verifica Σ' .

Teorema 1. — *El inverso a la derecha x' de x respecto a e , es también inverso a la izquierda.*

Por hipótesis, $xx' = e$. Pongamos $x'x = y$. Tendremos:

$$y^2 = x'xx'x = x'ex = x'x = y,$$

y es, pues, *idempotente*. Por otra parte, y tiene un inverso a la derecha y' , lo que permite escribir:

$$y^2y' = yy' = e.$$

Ahora bien,

$$y^2y' = ye = y$$

de donde, finalmente, $y = e$.

Teorema 2. — *El elemento unidad a la derecha e de D es también elemento unidad a la izquierda.*

En efecto, tenemos

$$ex = (xx')x = x(x'x) = xe = x.$$

El sistema Σ' implica, pues, como consecuencia el sistema Σ y la equivalencia lógica de los dos sistemas queda así establecida.

Puede utilizarse, desde luego, el sistema simétrico

$$\Sigma'' \left\{ \begin{array}{l} \text{I, asociatividad de la ley de composición;} \\ \text{II'', existe al menos un elemento neutro a la izquierda;} \\ \text{III'', con relación a ese elemento, todo elemento } x \text{ admite al menos un in-} \\ \text{verso a la izquierda.} \end{array} \right.$$

Otro sistema de axiomas muy importante hace intervenir la *existencia de cocientes* (pero no su unicidad, que aparecerá como consecuencia).

$$\Sigma_1 \left\{ \begin{array}{l} \text{I, } G \text{ es un semigrupo;} \\ \text{Ia, } G \text{ no es vacío;} \\ \text{V', Existencia de cocientes: cualesquiera que sean } a \text{ y } m \in G, \text{ existe al} \\ \text{menos un cociente a la derecha } x, \text{ y al menos un cociente a la iz-} \\ \text{quierda } y, \text{ de } m \text{ por } a, \text{ soluciones de } ax = m, ya = m, \text{ respectiva-} \\ \text{mente.} \end{array} \right.$$

Como se ha visto el sistema Σ implica la propiedad V (existencia y unicidad de los cocientes), por consiguiente V' , y por tanto Σ_1 . Recíprocamente:

Teorema 3. — *Un conjunto G con una ley de composición interna que cumple los axiomas del sistema Σ_1 es un grupo.*

Por hipótesis, G no es vacío; sea pues a un elemento de G . Según V' (donde tomamos $m = a$) existe al menos un elemento e de G tal que $ae = a$. Demostremos que e es elemento *neutro a la derecha*, es decir que $xe = x$ cualquiera que sea $x \in G$. Basta advertir que existe un elemento r tal que $x = ra$, lo que permite escribir

$$xe = (ra)e = r(ae) = ra = x.$$

Vemos así que el axioma II' se verifica. III' se cumple también, pues sólo es un caso particular de V' (un inverso a la derecha x' de x es un cociente a la derecha de e por x).

Notemos en fin, que los *grupos finitos* pueden ser caracterizados por el sistema de axiomas:

$$\Sigma_2 \left\{ \begin{array}{l} \text{I, } G \text{ es un semigrupo;} \\ \text{Ib, } G \text{ es un conjunto finito (no vacío);} \\ \text{IV, la regla de simplificación es válida en } G. \end{array} \right.$$

Todo grupo finito tiene estas propiedades; bastará, pues, establecer la proposición siguiente.

Teorema 4. — *Todo semigrupo finito $G (\neq \emptyset)$ en que se cumple la regla de simplificación es un grupo.*

Según IV, en la tabla de multiplicación de G , todo elemento figura a lo

sumo una vez en cada línea y en cada columna, luego exactamente una vez, puesto que G es finito. Esto implica la existencia y unicidad de cocientes, V , luego implica V' y G cumple el sistema de axiomas Σ_1 ; G es, pues, un grupo.

§ 3. Ejemplos de grupos

1. Entre los conjuntos de números usuales, muchos son grupos abelianos respecto a la adición o a la multiplicación. Citemos, *como grupos aditivos*:

el conjunto $\mathbf{Z}$ de los enteros de signo cualquiera,
 el conjunto $\mathbf{Q}$ de los racionales de signo cualquiera,
 el conjunto $\mathbf{R}$ de todos los números reales,
 el conjunto $\mathbf{C}$ de todos los números complejos;

y, como grupos multiplicativos:

el conjunto $\mathbf{Q}^+$ de los racionales positivos,
 el conjunto $\mathbf{R}^+$ de los reales positivos,
 el conjunto $\mathbf{C}_1$ de los números complejos de módulo 1,
 el conjunto $\mathbf{Q}^* = \mathbf{Q} - \{0\}$ de los racionales no nulos,
 el conjunto $\mathbf{R}^* = \mathbf{R} - \{0\}$ de los reales no nulos,
 el conjunto $\mathbf{C}^* = \mathbf{C} - \{0\}$ de los números complejos no nulos.

2. El semigrupo abeliano aditivo $\mathbf{Z}/(n)$ de las clases de restos módulo n es un *grupo*, puesto que tiene como elemento neutro la clase cero, y son opuestas las clases que contienen a ($0 \leq a \leq n-1$) y $n-a$. Este grupo, llamado *grupo aditivo de los enteros módulo n* , es finito y de orden n .

3. El conjunto $\mathcal{T}$ de las transformaciones de un conjunto E es, como hemos visto, un semigrupo, con la operación de composición $\circ$. Hay en $\mathcal{T}$ un *elemento neutro*, la transformación idéntica ϵ (definida por $\epsilon x = x$, $\forall x \in E$). Por otra parte, para toda transformación $\alpha \in \mathcal{T}$ y todo elemento x de E , existe en E un elemento x' , y uno sólo, tal que se tenga $\alpha x' = x$. La aplicación α' definida por

$$(\alpha') \quad x \rightarrow x' \quad \text{o} \quad \alpha' x = x',$$

o aplicación recíproca de α , es *inyectiva*, pues $\alpha' x = \alpha' y$ significa, llamando x' esta imagen común, $x = \alpha x'$, $y = \alpha x'$ luego exige $x = y$. Además α' es *exhaustiva* pues todo elemento x' de E es la imagen por α' de $x = \alpha x'$. La aplicación

α' es, pues, una transformación de E , *inversa* de α puesto que tenemos

$$(\alpha \circ \alpha')x = \alpha[\alpha'(x)] = \alpha x' = x \quad \forall x \in E$$

luego $\alpha \circ \alpha' = \epsilon$. Resulta que $\mathcal{G}$ es un grupo, designado frecuentemente por $\mathcal{S}(E)$. Cuando el conjunto E es *finito*, es cómodo distinguir sus n elementos con los subíndices $1, 2, \dots, n$, e incluso, confundir los elementos con sus índices: $E = \{1, 2, \dots, n\}$; las transformaciones α , que toman el nombre de *permutaciones* (o de *sustituciones*) se indican escribiendo:

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

donde $i_k = \alpha(k)$ es la imagen de k ¹. Hay, como se sabe $1 \cdot 2 \dots n = n!$ permutaciones distintas: el grupo constituido por todas ellas es pues, de orden $n!$; se le llama *grupo simétrico* y será designado por $\mathcal{S}_n$.

$\mathcal{S}_1$ se reduce a la transformación idéntica ϵ . Para $n = 2$, $\mathcal{S}_2$ consta de ϵ , y de la sustitución

$$\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

y su tabla se escribe

	ϵ	α
ϵ	ϵ	α
α	α	ϵ

$\mathcal{S}_2$ es abeliano.

$\mathcal{S}_3$ es de orden 6 y *no es abeliano*; en efecto, poniendo

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

tenemos

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

¹ En algunos autores, como en los más habituales libros en español, aparecen traspuestas las dos filas de la notación antedicha; y también el orden de los factores, que luego se dirá. (N. del T.)

N. B. — Para calcular $\alpha \circ \beta$ por ejemplo, se efectúa *primero* β , y después α : $(\alpha \circ \beta)(1) = \alpha[\beta(1)] = \alpha(3) = 3$, etc...

§ 4. Grupos asociados a otro dado, o a varios subgrupos. Subgrupos de un grupo

Hemos estudiado en Cap. II, § 1, diversos procedimientos que permiten construir nuevos semigrupos a partir de otro, o de varios semigrupos dados; supongamos ahora que el o los semigrupos dados, sean también grupos.

1.º Sea $\mathcal{F}$ el conjunto de las funciones f definidas en un conjunto X dado y tomando sus valores en un grupo dado, G , con notación multiplicativa y cuyo elemento neutro designaremos por e .

El producto fg de dos de tales funciones es por definición la función

$$x \rightarrow f(x)g(x) \quad (\forall x \in X)$$

Es claro que la función u que, para todo elemento x de X , toma el valor $u(x) = e$, es elemento neutro del semigrupo $\mathcal{F}$. La función f' definida por

$$f'(x) = [f(x)]^{-1} \quad \forall x \in X$$

verifica $ff' = f'f = u$; el conjunto $\mathcal{F}$ es pues un grupo.

2.º El producto $P = G_1 \times G_2$ de dos grupos multiplicativos en los que los respectivos elementos unidad son e_1, e_2 , es también un grupo con la multiplicación de pares (x_1, x_2) definida por

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2);$$

el par (e_1, e_2) es elemento neutro de P , y el par (x_1^{-1}, x_2^{-1}) es el inverso de (x_1, x_2) .

La propiedad subsiste en el caso $G_1 = G_2$, y se extiende inmediatamente a un número finito cualquiera k de grupos.

3.º Toda parte estable A de un grupo G es un semigrupo relativamente a la restricción a A de la ley de composición de G .

Definición. — Se llama *subgrupo* de G toda parte estable S de G que sea asimismo un grupo relativamente a la restricción a S de la ley de composición de G .

Si H es subgrupo de S y S subgrupo de G , entonces H es subgrupo de G .

Todo grupo G tiene al menos como subgrupos el mismo G y la parte $E = \{e\}$ constituida solamente por el elemento neutro. Un subgrupo S distinto de G y de E recibe el nombre de subgrupo *propio* (o verdadero).

Una parte estable no es, en general, un subgrupo. Así, en el grupo aditivo $\mathbf{Z}$ de los enteros relativos, el conjunto $\mathbf{N}$ de los enteros naturales es una parte estable, pero no es un subgrupo.

Si una parte estable A de un grupo G tiene, respecto a la correspondiente restricción de la ley de composición de G , un elemento idempotente e_A , en particular, un elemento neutro, se tiene, designando por e el elemento neutro de G y empleando la notación multiplicativa:

$$e_A^2 = e_A = e_A e,$$

de donde $e_A = e$. Si un elemento a de A tiene en A , con relación a e , un inverso a la derecha a' , o un inverso a la izquierda a'' , se tendrá, designando por a^{-1} el inverso de a en G :

$$aa' = e = aa^{-1} \quad a''a = e = a^{-1}a$$

luego, $a' = a^{-1}$, $a'' = a^{-1}$.

Por consiguiente, *todo subgrupo S de G contiene necesariamente el elemento neutro e de G , y si contiene al elemento x , también a su inverso x^{-1} .* Recíprocamente, *toda parte estable S que contenga a e y tal, que $x \in S$ implique $x^{-1} \in S$, es un subgrupo de G , puesto que S satisface a las condiciones Σ de definición de grupo.*

Como la condición $e \in S$ es consecuencia de que S sea una parte estable no vacía que si contiene a x también contiene a x^{-1} , podemos enunciar:

Teorema 1. — *Para que una parte no vacía S de un grupo G sea subgrupo de G , es necesario y suficiente que sea estable y que si contiene a un elemento x de G contenga también a su inverso x^{-1} .*

Según el teorema precedente, un subgrupo S debe contener con el par de elementos x, y , de G , al producto $x^{-1}y$. Ahora bien, esta condición necesaria es también suficiente para que una parte *no vacía* S sea un subgrupo. En efecto, sea s un elemento de $S (\neq \emptyset)$: tendremos, $s^{-1}s = e \in S$, luego $s^{-1}e = s^{-1} \in S$ y, en fin, si $s_1 \in S$, $(s^{-1})^{-1}s_1 = ss_1 \in S$; S es, pues, un subgrupo. Hemos demostrado así el teorema siguiente:

Teorema 2. — *Para que una parte no vacía S de G sea subgrupo de G , es necesario y suficiente que S contenga, al mismo tiempo que dos elementos x, y de G (distintos o no), el producto $x^{-1}y$.*

De esta condición necesaria y suficiente resulta, que cualquier intersección de subgrupos de G es un subgrupo de G , y en consecuencia, *el conjunto de los subgrupos de un grupo G es una familia de Moore.*

Pongamos $x^{-1}y = q$; q es el elemento (único) que verifica $xq = y$.

Por la condición del teorema 2:

$$x, y \in S, xq = y \ (q \in G) \text{ implican } q \in S,$$

Esto significa que S es, en G , una parte unitaria a la izquierda (cap. I, § 8). Así, en los grupos resultan coincidentes los subgrupos y las partes unitarias a la izquierda no vacías (y del mismo modo con las partes unitarias a la derecha, no vacías).

Ejemplos de subgrupos: 1. El centro Z de un grupo G es una parte estable (§ 1, teorema 4), *no vacía* ya que $e \in Z$. Si $z \in Z$, la igualdad $zx = xz$ trae consigo $xz^{-1} = z^{-1}x$, $\forall x \in G$, luego $z^{-1} \in Z$. Por consiguiente Z es un subgrupo de G . La igualdad $Z = G$ caracteriza los grupos abelianos.

2. En el grupo simétrico S_n , las n permutaciones de la forma

$$\sigma_k = \begin{pmatrix} 1 & 2 \dots n-k & n-k+1 \dots n \\ k+1 & k+2 \dots n & 1 \dots k \end{pmatrix}$$

($k = 0, 1, \dots, n-1$) se llaman permutaciones circulares. Se tiene $\sigma_0 = \epsilon$ (permutación idéntica), $\sigma_k \circ \sigma_h = \sigma_{k+h}$ si $k+h < n$, $\sigma_k \circ \sigma_h = \sigma_{k+h-n}$ si $k+h \geq n$, en particular $\sigma_k \circ \sigma_{n-k} = \epsilon$; las permutaciones circulares forman pues un subgrupo abeliano de orden n , C_n , del grupo simétrico S_n .

3. Consideremos un conjunto cualquiera E y el grupo $\mathcal{T}$ de las transformaciones de E (referente a la composición de las transformaciones $\circ$). A toda parte A de E podemos asociar:

a) el conjunto H_A de transformaciones τ que dejan fijo (o *invariante*) cada elemento de A :

$$\tau(a) = a \quad \forall a \in A$$

β) el conjunto Γ_A de las transformaciones σ que transforman el conjunto A en él mismo: $\sigma A = A$; Γ_A es un subgrupo de G ; H_A es un subgrupo de Γ_A , y por lo tanto también subgrupo de G .

4. El conjunto $\mathcal{P}(G)$ de las partes de un grupo G con la ley de composición definida a partir de la de G (Cap. I, § 4, 4.º) es un *semigrupo* (§ 1); siendo la parte vacía elemento lícito, $\mathcal{P}(G)$ no puede ser un grupo. Las partes no vacías

o complejos de G no forman tampoco, en general, un grupo. Tenemos en efecto, poniendo $E = \{e\}$.

$$G = EG$$

y

$$E \subseteq G, \quad \text{luego} \quad EG \subseteq G^2 \subseteq G,$$

de donde

$$EG = G^2 = G.$$

ahora bien, si G tiene más de un elemento, es $E \neq G$, luego la regla de simplificación no vale en el semigrupo $C = \mathcal{P}(G) - \{\emptyset\}$ que, por consiguiente, no es un grupo.

Designemos por H^- el conjunto de los inversos h^{-1} de los elementos h de H (se evita la notación H^{-1} porque en general, H^- no es inverso de H en C). Tenemos inmediatamente:

$$E \subseteq HH^-$$

$$(AB)^- = B^- A^-$$

y $A \subseteq B$ implica $A^- \subseteq B^-$.

Según el teorema 1, para que un complejo S de G sea un subgrupo, es necesario y suficiente que se tenga

$$S^2 \subseteq S \quad \text{y} \quad S^- \subseteq S.$$

Estas inclusiones exigen inmediatamente las igualdades correspondientes:

$$S^2 = S \quad \text{y} \quad S^- = S$$

puesto que $E \subseteq S$ implica $S = ES \subseteq S^2$ y $S^- \subseteq S$ implica

$$S = (S^-)^- \subseteq S^-.$$

Teorema 3. — *Para todo subgrupo S de un grupo G y para todo complejo K contenido en S se tiene:*

$$KS = S = SK.$$

La inclusión $K \subseteq S$ implica $KS \subseteq S^2 = S$; inversamente, si k es un elemento de K existe (según el axioma de los cocientes) para todo elemento s de

Sea un elemento x de S tal que $s = kx$; luego $S \subseteq KS$, de donde resulta la primera igualdad. La segunda se establece en forma análoga.

En particular si s es un elemento cualquiera de S se tiene: $sS = Ss = S$

§ 5. Homomorfismo en teoría de grupos; subgrupos distinguidos; descomposición en clases; automorfismos internos

Sea G un grupo y $\bar{G} = h(G)$ la imagen homomorfa de G en un homomorfismo h . Como sabemos (§ 1), $\bar{G}$ es un semigrupo. Además, la imagen $\bar{e} = h(e)$ del elemento unidad de G es elemento unidad de $\bar{G}$, y siendo $\bar{x}$ un elemento cualquiera de $\bar{G}$, x una de sus imágenes recíprocas en G , $h(x) = \bar{x}$, la imagen $h(x^{-1})$ es inversa de $\bar{x}$ en $\bar{G}$ (cap. I, § 6, teorema 1). Por consiguiente $\bar{G}$ es un grupo.

Teorema 4. — *La imagen homomorfa $\bar{G} = h(G)$ de un grupo G en un homomorfismo h es un grupo. El elemento unidad de $\bar{G}$ es la imagen del elemento unidad de G , teniéndose además*

$$h(x^{-1}) = [h(x)]^{-1} \quad (\forall x \in G)$$

Un subgrupo S de un grupo G se llama *subgrupo distinguido* de G (o *subgrupo invariante* de G , o *subgrupo normal* de G) si es permutable con cada elemento x de G , es decir si se tiene:

$$(1) \quad xS = Sx \quad \forall x \in G.$$

Escribiremos entonces $S \triangleleft G$.

Esta definición requiere las observaciones siguientes:

1.º La propiedad (1) significa que, cualquiera que sea $x \in G$, todo elemento de xS pertenece a Sx , e inversamente, luego que $\forall x \in G$ y $\forall s \in S$, se tiene:

$$xs \in Sx, \text{ es decir, } \exists s' \in S \text{ tal que } xs = s'x$$

e inversamente:

$$sx \in xS, \text{ es decir, } \exists s'' \in S \text{ tal que } sx = xs''.$$

2.º Para que S sea subgrupo distinguido de G , es suficiente (y evidentemente necesario) que se tenga:

$$(2) \quad xS \subseteq Sx \quad \forall x \in G.$$

Tendremos en efecto, reemplazando x por x^{-1}

$$x^{-1}S \subseteq Sx^{-1} \quad \forall x \in G$$

es decir (multiplicando los dos miembros a la izquierda y a la derecha por x)

$$Sx \subseteq xS \quad \forall x \in G$$

y, por consiguiente (1).

La condición (2) se escribe también:

$$xSx^{-1} \subseteq S \quad \forall x \in G$$

y significa que el elemento xSx^{-1} , al que se llama *transformado* de s por x , pertenece a S , para todo x en G y para todo s en S :

$$(2') \quad \forall x \in G \text{ y } \forall s \in S \quad xSx^{-1} \in S.$$

3.º Si S es un subgrupo distinguido de G y si H es un *grupo intermedio*:

$$S \subseteq H \subseteq G$$

S es, claro está, *subgrupo distinguido de H* . Pero si G' es un grupo que contiene a G como subgrupo propio

$$S \subseteq G \subset G'$$

no hay ninguna razón para que S , subgrupo de G' , sea distinguido en G' y, en general, no lo es.

4.º La familia $\mathcal{F}$ de subgrupos distinguidos de un grupo G es una familia de Moore, pues $G \in \mathcal{F}$ y si $\mathcal{F}'$ es una subfamilia de $\mathcal{F}$ y si

$$I = \bigcap_{S \in \mathcal{F}'} S$$

se tiene:

$$xix^{-1} \in S \quad \forall x \in G \quad \text{y} \quad \forall S \in \mathcal{F}'$$

luego

$$xix^{-1} \in I.$$

Ejemplos: Si G es un grupo abeliano, cualquier subgrupo S de G es subgrupo distinguido.

El centro Z de un grupo G es subgrupo distinguido de G ; se tiene, en efecto, $\forall z \in Z$ y $\forall x \in G$, $xzx^{-1} = z$. Se ve también que todo subgrupo del centro Z es un subgrupo distinguido de G .

Sea $\overline{G} = h(G)$ la imagen homomorfa de un grupo G en un homomorfismo h . Como hemos visto (§ 4, teorema 4) $\overline{G}$ es un grupo. Según el mismo teorema, la imagen $h(S) = \overline{S}$ de un subgrupo S de G es un subgrupo de $\overline{G}$.

Teorema 1. — Si S es subgrupo distinguido de G , su imagen homomorfa $h(S) = \overline{S}$ es un subgrupo distinguido de $\overline{G} = h(G)$.

Sean $\bar{x}$ un elemento cualquiera de $\overline{G}$, $\bar{s}$ un elemento cualquiera de $\overline{S}$ y x un elemento de G tal, que $h(x) = \bar{x}$; existe al menos un elemento s de S tal que $h(s) = \bar{s}$.

Tendremos por una parte $h(xs x^{-1}) = h(x) h(s) [h(x)]^{-1} = \bar{x} \bar{s} \bar{x}^{-1}$, y por otra parte $xs x^{-1} \in S$. Resulta pues, efectivamente, $\bar{x} \bar{s} \bar{x}^{-1} \in \overline{S}$ ($\forall \bar{x} \in \overline{G}$ y $\forall \bar{s} \in \overline{S}$).

Dado un elemento $\bar{x}$ de $\overline{G} = h(G)$, consideremos en G su imagen recíproca:

$$X = h^{-1}(\bar{x}) = \{ x ; x \in G, h(x) = \bar{x} \}$$

que es una clase de la partición asociada a la equivalencia de homomorfismo $\mathcal{H}$; se tiene en efecto (por definición)

$$(3) \quad x \equiv x_1(\mathcal{H}) \quad \text{si, y sólo si,} \quad (3') \quad h(x) = h(x_1).$$

Entre las clases X , a la que es imagen recíproca del elemento neutro $\bar{e}$ de $\overline{G}$, $N = h^{-1}(\bar{e})$ se le llama *núcleo* del homomorfismo h . Estudiemos las propiedades del núcleo N y de $\mathcal{H}$.

Desde luego $e \in N$; por otra parte, puesto que $\bar{e}$ es, en $\overline{G}$, elemento unidad a la derecha, su imagen recíproca N es, en G , un complejo unitario a la derecha (cap. I, § 8, teorema 7), luego N es un subgrupo de G (§ 4, comentarios al teorema 2).

La propiedad (3') que define la equivalencia de homomorfismo ($\mathcal{H}$) equivale a una u otra de las relaciones:

$$[h(x)]^{-1} h(x_1) = \bar{e}, \quad h(x_1) [h(x)]^{-1} = \bar{e}$$

que se escriben:

$$h(x^{-1}x_1) = \bar{e} \quad h(x_1x^{-1}) = \bar{e}$$

es decir:

$$(4) \quad x^{-1}x_1 \in N \quad (4') \quad x_1x^{-1} \in N$$

o, en fin:

$$x_1 \in xN \quad x_1 \in Nx$$

La clase X , módulo $\mathcal{H}$, que contiene un elemento cualquiera x de G , está pues, definida por:

$$(5) \quad X = xN = Nx$$

Tenemos pues:

$$xN = Nx \quad \forall x \in G.$$

y por consiguiente el núcleo N es un subgrupo distinguido de G . Enunciemos los resultados obtenidos:

Teorema 2. — *El núcleo N de un homomorfismo h que aplica un grupo G sobre un grupo $\bar{G} = h(G)$ es un subgrupo distinguido de G . La equivalencia de homomorfismo $\mathcal{K}$ viene definida mediante el núcleo N por*

$$x \equiv x_1(\mathcal{K}) \quad \text{si} \quad x^{-1}x_1 \in N \quad \text{o si} \quad x_1x^{-1} \in N.$$

La clase X , módulo $\mathcal{K}$ que contiene el elemento x de G es el complejo:

$$X = xN = Nx.$$

Recordemos que la equivalencia de homomorfismo $\mathcal{K}$ es compatible con la ley de composición de G , indicada aquí multiplicativamente (cap. I, § 6, teorema 2).

Caso particular: Supongamos dada en un grupo G , una equivalencia $\mathcal{R}$ compatible con la ley de composición de G y consideremos el homomorfismo canónico:

$$(h) \quad G \sim G/\mathcal{R}$$

que asocia a cada elemento x de G la clase $h(x) = X$, módulo $\mathcal{R}$, que contiene a x . El conjunto cociente $G/\mathcal{R}$ (cap. I, § 6) imagen del grupo G en el homomorfismo h , es asimismo un grupo, llamado grupo cociente. El elemento unidad E de $G/\mathcal{R}$ es la imagen $h(e)$ del elemento unidad e de G , en tanto que el subconjunto de G , $E = h(e)$ es por una parte la clase unidad, es decir la clase módulo $\mathcal{R}$ que contiene el elemento unidad e de G , por otra parte el núcleo del homomorfismo h , luego un subgrupo distinguido de G . Así:

Teorema 3. — *El conjunto cociente $G/\mathcal{R}$ de un grupo G por una relación de equivalencia $\mathcal{R}$ compatible con la ley de composición de G es un grupo, imagen de G en el homomorfismo canónico h , llamado grupo cociente de G por $\mathcal{R}$; la clase unidad E , núcleo de h , es un subgrupo distinguido de G . La clase X módulo $\mathcal{R}$ que contiene a x queda definida a partir de E por:*

$$X = xE = Ex.$$

Consideremos ahora, en un grupo G , una equivalencia $\mathcal{R}'$ que suponemos solamente regular a la derecha. No es ya posible hablar de ley de composición interna asociada en el conjunto cociente, pero todavía se tiene la proposición siguiente.

Teorema 4. — *En un grupo G , la clase unidad E' , módulo una equivalencia $\mathcal{R}'$ regular a la derecha, es un subgrupo de G y la clase X' módulo $\mathcal{R}'$, que*

contiene a un elemento x viene definida a partir de E' por:

$$X' = E'x.$$

Sean m_1, m_2 dos elementos de E' ; tenemos

$$m_1 \equiv e \equiv m_2 \quad (\mathcal{R}')$$

de donde, multiplicando a la derecha por m_2^{-1} :

$$m_1 m_2^{-1} \equiv m_2^{-1} \equiv e \quad (\mathcal{R}')$$

y por consiguiente $m_1 m_2^{-1} \in E'$; luego E' es un subgrupo de G .

Las congruencias $x_1 \equiv x$ y $x_1 x^{-1} \equiv e (\mathcal{R}')$ se implican una a otra; luego la clase X' , que contiene a x está definida por:

$$x_1 \in X' \quad \text{si, y sólo si} \quad x_1 x^{-1} \in E',$$

de donde

$$X' = E'x.$$

Inversamente, a un subgrupo cualquiera H de un grupo G , asociemos la relación binaria:

$$x \mathcal{R}'_H x_1 \quad \text{si, y sólo si,} \quad x_1 x^{-1} \in H.$$

Esta relación $\mathcal{R}'_H$ es *reflexiva* (pues $xx^{-1} = e \in H$), *simétrica* ($x_1 x^{-1} \in H$ implica $xx_1^{-1} = (x_1 x^{-1})^{-1} \in H$), *transitiva* ($x_2 x_1^{-1} \in H$ y $x_1 x^{-1} \in H$ implican $x_2 x^{-1} \in H$), es por lo tanto una relación de equivalencia. La clase X' módulo $\mathcal{R}'_H$, que contiene al elemento x es, según la definición de $\mathcal{R}'_H$, el complejo Hx .

Se tiene por tanto,

$$x_1 = x. \quad (\mathcal{R}'_H) \text{ si y sólo si } Hx = Hx_1$$

y, en consecuencia, $\mathcal{R}'_H$ es regular a la derecha.

Simétricamente, si consideramos la relación $\mathcal{R}''_H$ definida por $x \mathcal{R}''_H x_1$ si, y sólo si $x^{-1} x_1 \in H$ vemos que se trata de una *equivalencia regular a la izquierda*, y la clase X'' , módulo $\mathcal{R}''_H$, que contiene al elemento x es el complejo xH .

Tanto con módulo $\mathcal{R}'_H$ como con módulo $\mathcal{R}''_H$, la clase que contiene al elemento unidad e es el mismo subgrupo H . La partición de G definida por $\mathcal{R}'_H$ se llama *descomposición en clases a la derecha* $X' = Hx$; y, simétricamente, la partición definida por $\mathcal{R}''_H$ se designa *descomposición en clases a la izquierda* $X'' = xH$.¹

Hemos obtenido el teorema siguiente:

¹ A estas clases algunos autores las llaman *cogrupos* o, también, *clases de restos*. (N. del T.)

Teorema 5. — *A todo subgrupo H de G viene asociada una equivalencia regular a la derecha $\mathcal{R}_H'$, que define una descomposición en clases a la derecha $X' = Hx$, y una equivalencia regular a la izquierda $\mathcal{R}_H''$, que define una descomposición en clases a la izquierda $X'' = xH$.*

Para que un subgrupo S de G sea *distinguido* es necesario y suficiente que sea $xS = Sx$ para todo $x \in G$, esto es, que las clases $X' = Sx$ módulo $\mathcal{R}_S'$ y $X'' = xS$ módulo $\mathcal{R}_S''$, que tienen el elemento común x , coincidan; es decir, que las dos relaciones $\mathcal{R}_S', \mathcal{R}_S''$ se reduzcan a una sola: designaremos en adelante por $\mathcal{R}_S$ a esta relación, que por ser regular a la derecha y a la izquierda, es compatible con la ley de composición de G . El conjunto cociente $G/\mathcal{R}_S$ es el grupo imagen homomorfa de G en el homomorfismo canónico (Teorema 3) y S , clase unidad, es el *núcleo* de este homomorfismo. Podemos pues enunciar:

Teorema 6. — *A cada subgrupo distinguido S de G viene asociada una equivalencia $\mathcal{R}_S$ compatible con la ley de composición de G , tal que la clase módulo $\mathcal{R}_S$ que contiene un elemento x sea el complejo $xS = Sx (= X)$, S es el núcleo del homomorfismo canónico h que aplica G sobre el grupo cociente $G/\mathcal{R}_S$.*

Se ve finalmente, que la determinación de las imágenes de un grupo G , la de los subgrupos distinguidos de G y la de las equivalencias compatibles con la ley de composición de G , son problemas equivalentes. El conjunto de los grupos homomorfos, el de los subgrupos distinguidos y el de las equivalencias regulares se corresponden biunívocamente. Si S es un subgrupo distinguido de G se designa simplemente con G/S el grupo cociente $G/\mathcal{R}_S$ de G por la equivalencia regular $\mathcal{R}_S$ definida a partir de S .

Examinemos la forma que toma, en el caso de los grupos, el *teorema de homomorfismo* (cap. I, § 6, teorema 3). Sea $\bar{G} = h(G)$ la imagen de un grupo G en un homomorfismo h , que puede ser dado como un homomorfismo de G en un conjunto multiplicativo G' , que contenga a $\bar{G}$. Designemos como en el capítulo I, por $\bar{h}$ el homomorfismo correspondiente que aplica G sobre $\bar{G}$:

$$(\bar{h}) \quad G \sim \bar{G} = \bar{h}(G) = h(G).$$

La equivalencia de homomorfismo $\mathcal{R}$ es compatible con la ley de composición de G y se tiene el isomorfismo:

$$(i) \quad \bar{G} \simeq G/\mathcal{R}$$

donde

$$(6) \quad i(\bar{x}) = X = \{x; \bar{h}(x) = \bar{x}\}.$$

En particular $i(\bar{e}) = N$ es el *núcleo* del homomorfismo considerado y $G/\mathcal{R}$ es el grupo cociente de G por el subgrupo distinguido N . Por tanto:

Teorema 7. — *Toda imagen homomorfa $\overline{G}$ de un grupo G es isomorfa al grupo cociente G/N de G por el subgrupo distinguido N , núcleo del homomorfismo. Este isomorfismo i , que aplica $\overline{G}$ sobre G/N , definido por la fórmula (6) se llama *canónico*:*

$$(i) \quad \overline{G} \simeq G/N.$$

Para simplificar las notaciones, supondremos ahora que h es un homomorfismo que aplica G sobre $\overline{G}$.

Consideremos en la imagen homomorfa $\overline{G} = h(G)$, un subgrupo $\overline{S}$; nos proponemos estudiar su imagen recíproca en el grupo G .

$$S = h^{-1}(\overline{S}) = \{s; s \in G, h(s) \in \overline{S}\}.$$

Teorema 8. — *La imagen recíproca S de un subgrupo $\overline{S}$ de $\overline{G}$ contiene el núcleo N del homomorfismo h ; además S es subgrupo de G .*

Puesto que $\bar{e} \in \overline{S}$, se tiene $h^{-1}(\bar{e}) \subseteq h^{-1}(\overline{S})$, es decir $N \subseteq S$. Si s y s_1 son dos elementos de S se tiene:

$$h(s^{-1}s_1) = [h(s)]^{-1} h(s_1) \in \overline{S}, \quad \text{por tanto } s^{-1}s_1 \in h^{-1}(\overline{S}) = S,$$

y S es en efecto un subgrupo de G .

Supongamos ahora que $\overline{S}$ sea subgrupo *distinguido* de $\overline{G}$: sería fácil demostrar directamente que S es subgrupo *distinguido* de G . Nosotros obtendremos este resultado, con complementos importantes, aplicando el primer teorema de isomorfismo (cap. I, § 6, teor. 5).

Consideremos los dos homomorfismos (que aquí son epimorfismos)

$$(h) \quad G \sim \overline{G} = h(G) \quad (h') \quad \overline{G} \sim \overline{G}/\overline{S} = h'(\overline{G})$$

y el homomorfismo compuesto $f = h' \circ h$:

$$(f) \quad G \sim \overline{G}/\overline{S} = f(G).$$

Se deduce el isomorfismo:

$$(j) \quad f(G) = \overline{G}/\overline{S} \simeq G/\rho$$

donde ρ , equivalencia asociada al homomorfismo f , es compatible con la ley de composición de G .

El grupo cociente G/ρ se escribe G/S donde S designa, por ahora, la clase de unidad módulo ρ , *núcleo del homomorfismo* $f = h' \circ h$. S , subgrupo distinguido de G , será, pues, el conjunto de los elementos de G que h aplica sobre el núcleo de h' , es decir, sobre $\overline{S}$: así que, en efecto, S es la *imagen recíproca* $h^{-1}(\overline{S})$. Así tendremos el isomorfismo:

$$(j) \quad \overline{G}/\overline{S} \simeq G/S, \quad \text{donde } S = h^{-1}(\overline{S}).$$

Puesto que S es el núcleo de f , el isomorfismo (j) es también el que se obtiene aplicando a f el teorema de homomorfismo.

La clase $\bar{X} \in \bar{G}/\bar{S}$ tiene por imagen $j(\bar{X})$ la clase $X \in G/S$, conjunto de los elementos x de G tales que $\bar{X} = f(x) = h[h(x)] = \bar{S} h(x)$, según la significación de (h') ; así,

$$(7) \quad X = j(\bar{X}) = Sx \text{ si } \bar{X} = \bar{S}\bar{x}, \text{ con } \bar{x} = h(x).$$

Consideremos ahora los grupos cocientes G/N , G/S de G respecto a los subgrupos *distinguidos*, N , S con $N \subseteq S (\subseteq G)$ (y que podrían, en lo que sigue, ser dados *a priori*). A cada clase $X_1 = Nx \in G/N$, asociamos la clase $X = Sx = SNx = SX_1$ que es además la clase, con respecto a S , que incluye a X_1 . La aplicación φ de G/N sobre G/S así definida es un *homomorfismo*; en efecto, sea $Y_1 = Ny \in G/N$; tenemos:

$$X_1 Y_1 = NxNy = Nxy$$

y por consiguiente:

$$\varphi(X_1 Y_1) = \varphi(Nxy) = Sxy = SxSy = XY = \varphi(X_1)\varphi(Y_1).$$

El núcleo Λ del homomorfismo φ es el conjunto de las clases Nx tales que $Sx = S$, clase unidad, lo que se verifica si $x \in S$ y solamente en este caso. Λ conjunto de clases Ns , donde s recorre S , es pues el grupo cociente S/N y tenemos el isomorfismo:

$$(j_1) \quad G/S \simeq G/N/S/N$$

siendo j_1 la aplicación que a $X = Sx \in G/S$, asocia $(S/N) X_1 \in G/N/S/N$, donde $X_1 = Nx$:

$$(8) \quad j_1(X) = (S/N) X_1$$

si $X = Sx$ y $X_1 = Nx$.

Enunciemos el teorema fundamental obtenido:

Teorema 9 (primer teorema de isomorfismo para grupos). — Dado un homomorfismo h que aplica un grupo G sobre un grupo $\bar{G}$,

$$(h) \quad G \sim \bar{G} = h(G)$$

la imagen recíproca $S = h^{-1}(\bar{S})$ de un subgrupo distinguido $\bar{S}$ de $\bar{G}$ es un subgrupo distinguido S de G que contiene al núcleo N de h , y se tienen los isomorfismos:

$$\bar{G}/\bar{S} \simeq G/S \simeq G/N/S/N.$$

Estos isomorfismos j y j_1 están definidos respectivamente por (7) y por (8).

Además, el isomorfismo j_1 se puede establecer para cualquier par S, N de subgrupos distinguidos de G tales que $N \subseteq S$.

En fin cualquier subgrupo distinguido S de G que contenga a N tiene en $\bar{G} = h(G)$, una imagen $h(S)$, subgrupo distinguido de $\bar{G}$ (teorema 1), cuya imagen recíproca $h^{-1}[h(S)]$ es la reunión de las clases Ns cuando s describe o recorre S ; esta reunión no es otra que $NS = S$. Tenemos pues una correspondencia biyectiva

$$h^{-1} \quad \bar{S} \rightarrow h^{-1}(\bar{S}) = S$$

entre los subgrupos distinguidos $\bar{S}$ de $\bar{G}$ y los subgrupos distinguidos S de G que contienen al núcleo N de h .

Para obtener otras propiedades importantes, ligadas a otra aplicación del teorema del homomorfismo, volvamos a una de las definiciones de subgrupo distinguido: S es subgrupo distinguido de G si

$$(2') \quad \forall a \in G \quad y \quad \forall s \in S \quad asa^{-1} \in S$$

Fijado un elemento a , consideremos la aplicación α de G en sí mismo que asocia cada x de G con su transformado por a :

$$(\alpha) \quad x \rightarrow axa^{-1} = \alpha(x).$$

Por la regla de simplificación α es una aplicación inyectiva; y puesto que

$$\alpha(a^{-1}x'a) = aa^{-1}x'aa^{-1} = x',$$

α es exhaustiva; luego α es una aplicación biyectiva de G sobre sí mismo. Además, tenemos

$$\alpha(xy) = axya^{-1} = axa^{-1} \cdot aya^{-1} = \alpha(x) \alpha(y);$$

por lo que α es, en fin, un automorfismo de G ; los automorfismos α , ... así definidos a partir de los elementos a , ... de G son los llamados automorfismos internos.

Teorema 10. — El conjunto Γ de los automorfismos internos de un grupo G es un grupo, imagen homomorfa de G . Γ es isomorfo al grupo cociente G/Z de G por su centro Z .

Consideremos la aplicación

$$(\varphi) \quad a \rightarrow \alpha = \varphi(a)$$

de G sobre Γ ; $\varphi(ab)$ es el automorfismo interno

$$x \rightarrow (ab) x(ab)^{-1} = a(bxb^{-1}) a^{-1} = (\alpha \circ \beta)x$$

luego $\varphi(ab) = \varphi(a) \circ \varphi(b)$ y φ es un homomorfismo que aplica G sobre Γ ; por lo tanto Γ es un grupo.

Según el teorema de homomorfismo, se tiene el isomorfismo

$$\Gamma \simeq G/N$$

donde N es el núcleo del homomorfismo φ , es decir el conjunto de los elementos n de G a los que corresponde, como automorfismo interno, el automorfismo idéntico:

$$n x n^{-1} = x \quad \forall x \in G.$$

La igualdad precedente se escribe $n x = x n$ y expresa que n conmuta con todos los elementos de G : N no es, pues, otra cosa que el centro Z de G , lo que concluye la demostración.

La definición (2') de subgrupo distinguido S de G se escribe:

$$(2'') \quad \alpha(S) \subseteq S \quad \forall \alpha \in \Gamma$$

propiedad, señalemos, equivalente a:

$$\alpha(S) = S \quad \forall \alpha \in \Gamma$$

como se ve aplicando el automorfismo α^{-1} a los dos miembros de (2''). Los subgrupos distinguidos de un grupo G son los subgrupos transformados en sí mismos por todo automorfismo interno de G . De aquí el nombre de subgrupos invariantes con que también se designa a esos subgrupos.

La imagen $\alpha(H) = a H a^{-1}$ de un subgrupo cualquiera H por un automorfismo interno, es también un subgrupo de G , al que se llama *conjugado* de H .

Veamos finalmente algunas propiedades, que se refieren a la descomposición de un grupo G en clases a la derecha $X' = Hx$ o en clases a la izquierda $X'' = xH$ con relación a un subgrupo cualquiera. Según la regla de simplificación, a dos elementos distintos h, h_1 de H corresponden en X' dos elementos distintos hx, h_1x ; lo mismo en X'' . Cualquier clase, a la derecha o a la izquierda, se corresponde pues biyectivamente con el subgrupo H , en otros términos, *tiene la misma potencia que H* . Si H es finito y tiene n elementos, todas las clases $X' = Hx$ o $X'' = xH$ también tienen n elementos.

La clase a la izquierda $X'' = xH$ relativa al subgrupo H puede ponerse bajo la forma:

$$X'' = (x H x^{-1}) x.$$

Esto es la clase a la derecha que contiene a x en la descomposición de G relativa al subgrupo $x H x^{-1}$, conjugado de H . Esta propiedad implica el hecho de que para un subgrupo distinguido, es decir, que coincida con sus conjugados, la clase a la derecha X' y la clase a la izquierda X'' coinciden totalmente en cuanto tengan un elemento común x .

El conjunto $(Hx)^{-} = x^{-1} H^{-} = x^{-1} H$ de los inversos de los elementos de la clase a la derecha con x , es la clase a la izquierda con x^{-1} , respecto a H , lo que define una correspondencia biyectiva entre el conjunto de las clases a la derecha

$$G/\mathcal{R}'_H = \{ H, \dots, X', \dots \}$$

y el conjunto

$$G/\mathcal{R}_H'' = \{ H, \dots, X'', \dots \}$$

de las clases a la izquierda distintas respecto a H . Esos dos conjuntos tienen la misma potencia; si uno de ellos es finito, el otro lo es también y tienen ambos el mismo número de elementos. El número i (finito o infinito) de clases en cualquiera de las dos descomposiciones de G relativa a su subgrupo H , es por definición el índice de H en G .

Si G es un grupo de orden finito N , el orden n y el índice i de H son evidentemente finitos y se tiene

$$N = in$$

puesto que las i clases distintas X' tienen n elementos cada una.

Teorema 11 (Lagrange). — El orden n de un subgrupo H de un grupo G de orden finito es divisor del orden N de este grupo.

Corolario. — Un grupo G de orden p primo no tiene subgrupos propios.

§ 6. Leyes de composición externa. Espacios homogéneos. Teoremas de Sylow

Definición. — Dados un conjunto E y un segundo conjunto Ω al que llamaremos *dominio de operadores*, una ley de composición externa a la izquierda, en E , es, como hemos visto en § 2, una aplicación del conjunto producto $\Omega \times E$ en E . La imagen del par $(\omega, x) \in \Omega \times E$ se indica de ordinario por $\omega * x$, en notación multiplicativa, ωx .

Los elementos $\omega, \dots$ de Ω se llaman *operadores*; dado un elemento x de E , el conjunto

$$X = \{ \omega * x, \omega \in \Omega \}$$

es la *trayectoria* de x . La denotaremos también por $\Omega * x$.

A cada operador $\omega \in \Omega$, asociemos la *aplicación* φ de E en sí mismo, definida por

$$(1) \quad \varphi(x) = \omega * x, \quad (x \in E).$$

El operador ω se dice *inyectivo* si la correspondiente aplicación φ es inyectiva, esto es, cuando

$$x_1 \neq x_2 \quad \text{implica} \quad \omega * x_1 \neq \omega * x_2$$

(o si $\omega * x_1 = \omega * x_2$ implica $x_1 = x_2$); análogamente, ω es *suprayectivo* si φ es suprayectiva (o sobre), es decir, si

$$\forall y \in E, \quad \exists x \in E \quad \text{tal que} \quad \omega * x = y;$$

en fin, ω es *biyectivo* si es a la vez inyectivo y suprayectivo. El dominio de operadores Ω se dice asimismo *biyectivo* cuando todo elemento ω de Ω es biyectivo.

Asociando a cada operador ω la aplicación φ de E en E definida en lo anterior, obtenemos una aplicación α de Ω en el conjunto $\mathcal{A}(E)$ de las aplicaciones de E en E ; si Ω es biyectivo, α es una aplicación de E perteneciente al conjunto $\mathcal{S}(E)$ de las biyecciones de E . Escribiremos

$$\varphi = \alpha(\omega).$$

Si la aplicación α es inyectiva, es decir, si dos operadores ω_1 y ω_2 distintos (en tanto que elementos de Ω) originan aplicaciones φ_1 y φ_2 distintas, diremos que el dominio Ω es *reducido*.

Dos aplicaciones $\varphi_1 = \alpha(\omega_1)$, $\varphi_2 = \alpha(\omega_2)$ se componen según la fórmula

$$(2) \quad (\varphi_2 \circ \varphi_1)(x) = \varphi_2[\varphi_1(x)] = \omega_2 * (\omega_1 * x)$$

Un caso importante es aquel en el que el dominio de operadores Ω posee una ley de composición interna, que denotaremos $\cdot$, y la aplicación α de Ω en $\mathcal{A}(E)$ es un homomorfismo relativo a las leyes $\cdot$ de Ω y $\circ$ de $\mathcal{A}(E)$:

$$(3) \quad \alpha(\omega_2 \cdot \omega_1) = \alpha(\omega_1) \circ \alpha(\omega_2) = \varphi_2 \circ \varphi_1, \quad \forall \omega_1, \omega_2 \in \Omega.$$

Ahora, $\alpha(\omega_2 \cdot \omega_1)$ es la aplicación φ asociada a $\omega_2 \cdot \omega_1$, definida, pues, por

$$\varphi(x) = (\omega_2 \cdot \omega_1) * x \quad \forall x \in E;$$

por tanto, la condición (3), $\varphi = \varphi_2 \circ \varphi_1$, se escribe

$$(\omega_2 \cdot \omega_1) * x = (\varphi_2 \circ \varphi_1)(x)$$

es decir, teniendo en cuenta (2),

$$(4) \quad (\omega_2 \cdot \omega_1) * x = \omega_2 * (\omega_1 * x), \quad \forall x \in E \quad \text{y} \quad \forall \omega_1, \omega_2 \in \Omega.$$

Esta condición necesaria y suficiente para que α sea un homomorfismo de Ω en $\mathcal{A}(E)$, hace intervenir sólo los elementos de E y los de Ω ; se la designa por *condición de asociatividad mixta*. Si Ω es *biyectivo*, se tiene un homomorfismo de Ω en el grupo de las biyecciones $\mathcal{S}(E)$; si Ω es *reducido*, Ω es *isomorfo* a su imagen $\alpha(\Omega)$.

Cuando el dominio de operadores Ω con la ley $\cdot$, posee un elemento neutro ε , diremos que ε es *operador unidad* si la aplicación $\alpha(\varepsilon)$ es la aplicación idéntica I_E de E sobre E , es decir, cuando

$$(5) \quad \forall x \in E, \quad \varepsilon * x = x$$

Nota. — Si el dominio de operadores Ω verifica la condición de asociatividad mixta (4), si admite un elemento neutro a la derecha ε , y si contiene al menos un operador inyectivo ω , ε es operador-unidad.

En efecto, con esas hipótesis tenemos,

$$\forall x \in E, \quad \omega * x = (\omega \cdot \varepsilon) * x = \omega * (\varepsilon * x)$$

de donde

$$x = \varepsilon * x.$$

Definición. — Si Ω es un grupo (para la operación $\cdot$), y si la aplicación α es un homomorfismo de Ω en el grupo $\mathcal{S}(E)$ de las biyecciones de E , se dice que el grupo Ω opera en el conjunto E . De hecho, no es necesario que el grupo se dé como un dominio de operadores. Cualquier grupo abstracto G que admita una imagen homomorfa en el grupo de las biyecciones de E es un grupo que opera en E . En efecto, si para cada elemento g de G ponemos

$$\alpha(g) = \varphi \in \mathcal{S}(E) \quad \text{y} \quad g * x = \varphi(x) \quad \forall x \in E,$$

se hace de g un operador biyectivo, α tiene la misma significación que en lo anterior y es, por hipótesis, un homomorfismo.

Si Ω opera en E se cumple la condición (4) de asociatividad mixta. Además, la imagen homomorfa $\alpha(\Omega)$ tiene por elemento-unidad la imagen $\alpha(\varepsilon)$ del elemento neutro ε de Ω ; pero el elemento unidad del subgrupo $\alpha(\Omega)$ de $\mathcal{S}(E)$ es necesariamente el de $\mathcal{S}(E)$, es decir, la aplicación idéntica I_E ; por consiguiente, ε es operador-unidad [condición (5)].

Recíprocamente, si para un dominio de operadores Ω que es un grupo, se cumplen las condiciones (4) y (5), Ω opera en E .

En efecto, la condición de asociatividad mixta (4) implica que $\alpha(\Omega)$ es imagen homomorfa de Ω en $\mathcal{A}(E)$. Además, Ω es biyectivo: $\alpha(\Omega) \subseteq \mathcal{S}(E)$, pues la igualdad $y = \omega * x$ implica

$$\omega^{-1} * y = \omega^{-1} * (\omega * x) = (\omega^{-1} \cdot \omega) * x = \varepsilon * x = x$$

luego ω es inyectivo, y puesto que también

$$\omega * (\omega^{-1} * y) = \varepsilon * y = y, \quad \Omega \text{ es suprayectivo.}$$

Propiedades. — 1) Si un grupo G opera en un conjunto E y si G' es un subgrupo de G , también G' opera en E , puesto que $\alpha(G')$ subgrupo de $\alpha(G)$, es también un subgrupo del grupo $\mathcal{S}(E)$ de las biyecciones de E .

2) Una parte A de E se dice invariante por G si se tiene $\omega * A = \varphi(A) = A$ para toda biyección $\varphi = \alpha(\omega)$ definida por cada operador $\omega \in G$. Cuando así

sucede, la restricción φ_A de φ a A es evidente una biyección de A sobre sí mismo, y G admite una imagen homomorfa en el grupo de las biyecciones de A . Vemos, pues, que *el grupo G opera también en toda parte A de E que sea invariante por G .*

3) Toda aplicación φ de E en E puede ampliarse a una aplicación Φ de $\mathcal{T}(E)$ en $\mathcal{T}(E)$ definida por

$$\Phi(A) = \{ \varphi(a) ; a \in A \}.$$

Si φ es suprayectiva, también evidentemente lo es Φ (se tiene $\Phi(X) = M$ al tomar para X la imagen recíproca de M). Si φ es inyectiva, también lo es Φ (pues $\Phi(A) = \Phi(B)$ implica por ejemplo $A \subseteq B$: si en efecto $a \in A$, $\varphi(a) \in \Phi(A) = \Phi(B)$, luego $\varphi(a) = \varphi(b)$, donde $b \in B$, de donde $a = b \in B$). Por consiguiente, si φ es biyectiva Φ lo es también, y *si un grupo G opera en E , entonces también opera en $\mathcal{T}(E)$.*

Finalmente, las tres propiedades precedentes implican que *si un grupo G opera en un conjunto E , todo subgrupo G' de G opera en $\mathcal{T}(E)$ y, más generalmente, en toda familia $\mathcal{F}$ de partes de E invariante por G' . Todo operador biyectivo ω transforma una parte finita A de E en una parte $\varphi(A)$ que tiene el mismo número de elementos, por lo que vemos que la familia $\mathcal{F}_n$ de las partes finitas que tienen un número dado n de elementos es invariante para todo subgrupo G' de un grupo G que opere en E : G' opera pues en esta familia $\mathcal{F}_n$, y también en la familia $\mathcal{F}'_n$ de las partes de E que tienen a lo más n elementos.*

4) Dado un grupo G que opera en un conjunto E , el conjunto G_a de los elementos g de G que dejan fijo un elemento a de E ,

$$g * a = a,$$

es un subgrupo de G : $g_1 \in G_a$ (y $g_2 \in G_a$ implican $g_1 g_2 \in G_a$ según (4), y si $g \in G_a$ también $g^{-1} \in G_a$ según (4) y (5). Este grupo G_a se llama el *estabilizador* del elemento a .

Estudiemos la trayectoria $G*a$ del elemento a por los diferentes operadores del grupo G . La igualdad

$$g_1 * a = g * a$$

equivale, según (4) y (5), a

$$g^{-1} * (g_1 * a) = (g^{-1} g_1) * a = a,$$

luego

$$g^{-1} g_1 \in G_a, \quad \text{es decir,} \quad g_1 \in g G_a.$$

lo que expresa que g_1 está en la misma clase a la izquierda que g en la descomposición de G en clases a la izquierda relativas al subgrupo G_a . En conclusión, podemos enunciar:

Teorema 1. — *Cuando un grupo G opera en un conjunto E , el conjunto de los elementos g de G para los que la imagen $\gamma(a) = g*a$ es un mismo elemento del conjunto E es una clase a la izquierda de G relativa al estabilizador G_a de a ; por consecuencia, la trayectoria $G*a$ de un elemento a de E se corresponde biyectivamente al conjunto de las clases a la izquierda de G relativas al estabilizador G_a de a .*

Corolario. — *Cuando G es un grupo de orden finito, el número de elementos de una trayectoria es divisor del orden del grupo G .*

Nota. — En el estudio anterior se puede sustituir el grupo G por su imagen homomorfa $\Gamma = \alpha(G)$ en el grupo $\mathcal{S}(E)$ de las biyecciones de E . Si Γ_a es el estabilizador de a en Γ , G_a es su imagen recíproca $\alpha^{-1}(\Gamma_a)$. La trayectoria de a corresponde biyectivamente al conjunto de las clases a la izquierda de Γ relativas a Γ_a . Se ve que si Γ_a tiene en Γ un índice finito, también G_a lo tiene en G , y estos dos índices son iguales.

Ejemplo 1. — Hemos considerado ya los *automorfismos internos* de un grupo G : a cada elemento s de G se asocia el automorfismo σ definido por

$$\sigma(x) = sx s^{-1}, \quad (x \in G).$$

Si escribimos

$$s * x = sx s^{-1} = \sigma(x)$$

hacemos de G un dominio de operadores $\Omega (= G)$ que opera en el conjunto $E = G$, pues el conjunto Σ de los automorfismos internos es imagen homomorfa de G en el grupo de biyecciones $\mathcal{S}(G)$ (§ 5, Teor. 10):

$$\alpha(\Omega) = \Sigma \simeq G/Z,$$

donde Z es el centro de G .

Al operar sobre sí mismo por los automorfismos internos, G no es en general un dominio de operadores reducido: para que dos elementos s_1, s_2 , den el mismo automorfismo interno σ , es necesario y suficiente que pertenezcan a la misma clase de descomposición de G relativa a su centro. Así, G es un dominio de operadores reducido si y sólo si su centro Z se reduce al elemento unidad e .

Advirtamos también que en el caso general, cada elemento z del centro Z es invariante para todo automorfismo interno:

$$\sigma(z) = szs^{-1} = zss^{-1} = z.$$

Ejemplo 2. — Tomemos como conjunto E un grupo G y como dominio de operadores Ω el propio grupo G . El producto externo $\omega * x$, donde $\omega = a \in G$, lo hacemos coincidir con el producto ordinario ax en el grupo G . La aplicación φ de G en sí mismo asociada al operador $\omega = a$ es la *traslación a la izquierda* γ_a :

$$\gamma_a(x) = ax$$

γ_a es una biyección, puesto que en el grupo G vale la regla de simplificación a la izquierda. En consecuencia, *todo grupo G opera sobre sí mismo por las traslaciones a la izquierda (y análogamente por las traslaciones a la derecha).*

Además, las traslaciones γ_a, γ_b correspondientes a dos elementos a, b , distintos son distintas: este dominio de operadores es, pues, *reducido*, y el grupo Γ de las traslaciones a la izquierda, subgrupo de $\mathcal{S}(E)$, es *isomorfo* a E .

Cuando G es finito, el resultado precedente se anuncia en una forma clásica:

Teorema 2 (teorema de Cayley). — *Todo grupo finito G de orden n es isomorfo a un subgrupo Γ del grupo simétrico $\mathcal{S}_n$.*

Otra propiedad importante del grupo de las traslaciones a la izquierda es que existe siempre una de ellas, γ_m , que transforma a un elemento dado a en otro elemento dado b ($m = ba^{-1}$). Ésta es una distinción importante entre este grupo y el de los automorfismos internos, para el que todo elemento del centro es invariante. De este modo estamos llevados a importantes definiciones, que vamos a enunciar, para simplificar la escritura, en notación multiplicativa (ga en vez de $g * a$).

Dado un grupo G que opera en un conjunto E , consideremos en E la relación binaria definida por

$$a \mathcal{G} b \quad \text{si existe} \quad g \in G \quad \text{tal que} \quad b = ga.$$

La relación $\mathcal{G}$ es *reflexiva* (porque el elemento unidad e del grupo G es operador unidad), es *simétrica* [pues $b = ga$ implica $a = ea = (g^{-1}g)a = g^{-1}(ga) = g^{-1}b$], es *transitiva* [pues si, además, $c = g_1b$ se tiene: $c = g_1(ga) = (g_1g)a$].

Por tanto, $\mathcal{G}$ es una relación de equivalencia, a la que se llama *equivalencia de transitividad*. Las clases módulos $\mathcal{G}$ se llaman *clases de transitividad*; según las definiciones, cada clase de transitividad es la trayectoria de uno cualquiera de sus elementos.

Si $\mathcal{G}$ es la *relación universal*, es decir, si para cada par de elementos a, b de E , existe al menos un elemento g en el grupo G tal que $b = ga$, se dice que G *opera transitivamente en E* , y que el ente (E, G) es un *espacio homogéneo*.

En caso contrario, $\mathcal{G}$ descompone a E en, por lo menos, *dos clases de transitividad*, $A, B, \dots$; se dice entonces que G *opera intransitivamente en el conjunto E* .

Cada clase de transitividad C es *invariante por G* , pues, para todo operador $g \in G$, la relación $c \in C$ implica $gc \in C$, de donde $\varphi(C) \subseteq C$; y considerando la biyección inversa $\varphi^{-1} = \alpha(g^{-1})$ tenemos análogamente $\varphi^{-1}(C) \subseteq C$.

de donde, tomando las imágenes de los dos miembros, $C \subseteq \varphi(C)$, por lo que vale la igualdad.

Finalmente, *el grupo G opera en cada clase de transitividad C y es claro que opera transitivamente: luego, (C, G) es un espacio homogéneo.*

Reconsideremos los ejemplos anteriores. Si se hace operar en sí mismo a un grupo G por las traslaciones a la izquierda (ejemplo 2), G opera transitivamente y nos encontramos ante un espacio homogéneo (G, G) .

Por el contrario, cuando G opera en sí mismo por los automorfismos internos (ejemplo 1), cada elemento del centro, en particular el elemento neutro e , es invariante y constituye una clase de transitividad; en cuanto G tiene más de un elemento opera intransitivamente en sí mismo, pero G opera transitivamente en cada clase de transitividad: una tal clase X es el conjunto de los elementos sxs^{-1} ($s \in G$) conjugados de un elemento dado x ($x \in X$).

Vamos ahora a estudiar sucesivamente los espacios homogéneos y los conjuntos en los que opera (intransitivamente) un grupo G .

Espacios homogéneos. — Sea (E, G) un espacio homogéneo (el grupo G opera transitivamente en el conjunto E). Designaremos por Γ la imagen homomorfa de G en el grupo $\mathcal{S}(E)$ de las biyecciones de E , y por $\gamma = \alpha(g)$ la biyección determinada por el elemento g del grupo G . Para un segundo espacio homogéneo (E', G') adoptaremos las notaciones correspondientes: $\Gamma', \gamma' = \alpha(g')$, donde $g' \in G'$.

El espacio homogéneo (E', G') se dirá *imagen homomorfa* del espacio homogéneo (E, G) si existen:

- 1) Una suprayección η de E sobre E' : $E' = \eta(E)$;
- 2) Un homomorfismo h de G sobre G' : $G' = h(G)$, tales que sea:

$$(6) \quad \forall g \in G \quad \eta \circ \gamma = \gamma' \circ \eta$$

donde $\gamma = \alpha(g)$, $\gamma' = \alpha(g')$, $g' = h(g)$; esta condición se expresa diciendo que el diagrama

$$\begin{array}{ccc} E & \xrightarrow{\gamma} & E \\ \eta \downarrow & & \downarrow \eta \\ E' & \xrightarrow{\gamma'} & E' \end{array}$$

es *conmutativo*. Si se vuelve a los elementos de E y de G la condición (6) toma la forma

$$(6') \quad \forall g \in G \quad \text{y} \quad \forall x \in E, \quad \eta(gx) = h(g) \eta(x).$$

Si, además, η es una biyección y h es un isomorfismo, se dice que los dos espacios homogéneos (E, G) y (E', G') son *isomorfos*.

Tomemos, en particular, $E' = E$ y $G' = \Gamma = \alpha(g)$: es (E, Γ) imagen homomorfa de (E, G) , donde η es la aplicación idéntica I_E de E sobre sí mismo y el homomorfismo h no es otro que α .

Según (6'), las igualdades

$$(7) \quad \eta x = \eta x_1 \quad (x, x_1 \in E)$$

$$(8) \quad h(g) = h(g_1) \quad (g, g_1 \in G)$$

implican

$$(9) \quad \eta(g_1 x_1) = h(g_1) \eta(x_1) = h(g) \eta(x) = \eta(gx).$$

Ahora, los dos elementos g, g_1 de G que verifican (8) pertenecen a la misma clase C de la descomposición del grupo G relativa al núcleo N del homomorfismo h ; los elementos x, x_1 de E que verifiquen (7) pertenecen a la misma clase X de la descomposición del conjunto E respecto a la equivalencia de aplicación $\mathcal{A}$ de η . Según (9) es legítimo escribir

$$CX = Y,$$

donde $Y = \eta^{-1}[(gx)]$ es la clase módulo $\mathcal{A}$ conjunto de los elementos y de E que tienen la misma imagen gx : $\eta y = \eta(gx)$.

La aplicación $C \rightarrow g' = h(g)$ (donde $g \in C$) es un isomorfismo de G/N sobre G' , y la aplicación $X \rightarrow x' = \eta(x)$ (donde $x \in X$) es una biyección de $E/\mathcal{A}$ sobre E' en que la imagen de CX es $g'x'$, y por tanto, el grupo cociente G/N opera sobre el espacio cociente $E/\mathcal{A}$ de modo transitivo, y se tiene el isomorfismo de espacios homogéneos

$$(E/\mathcal{A}, G/N) \simeq (E', G').$$

Esta proposición constituye el *teorema de homomorfismo* para los espacios homogéneos.

Dados un espacio homogéneo (E, G) y dos elementos a, x de E , existe al menos un elemento g_0 del grupo G tal que

$$(10) \quad g_0 a = x$$

(puesto que G opera transitivamente en E) y, según el Teor. 1, el conjunto de los elementos g de G que cumplen la condición (10) es una clase a la izquierda, X , de G respecto al estabilizador G_a de a :

$$X = g_0 G_a$$

y el conjunto C_a de clases a la izquierda de G respecto a G_a es la imagen de la trayectoria de a (es decir, aquí, del mismo E) por la biyección β que asocia X a x :

$$(11) \quad \text{si} \quad x = g_0 a, \quad \beta(x) = X = g_0 G_a.$$

Ahora, el grupo G , operando en sí mismo por las traslaciones a la izquierda, opera también en $\mathcal{P}(G)$ y en toda parte de $\mathcal{P}(G)$ que sea invariante por las traslaciones a la izquierda; éste es el caso para todo conjunto $\mathcal{C}$ de clases a la izquierda $C = gS$ relativas a un subgrupo cualquiera S ($\forall t \in G$, $tC = (tg)S \in \mathcal{C}$) y, además, G opera transitivamente en $\mathcal{C}$ (puesto que $\forall C_1 = g_1S \in \mathcal{C}$, $(g_1G^{-1})C = C_1$). En particular, G opera transitivamente en el conjunto $\mathcal{C}_a$ de las clases a la izquierda relativas al estabilizador G_a , lo que hace de $(\mathcal{C}_a, G)$ un espacio homogéneo.

Establecido esto, la biyección β aplica $\mathcal{C}_a$ sobre E , y el automorfismo idéntico ε aplica G sobre sí mismo; además, cualesquiera sean $x \in E$ y $g \in G$, tendremos según (11), si $x = g_0a$,

$$gx = gg_0a \quad \text{luego} \quad \beta(gx) = gg_0G_a = gX = \varepsilon(g) \beta(x).$$

La condición (6') queda, pues, satisfecha, luego los espacios homogéneos $(\mathcal{C}_a, G)$ y (E, G) son isomorfos.

Como esta propiedad se verifica cualquiera sea el elemento a de E , resulta: *si a y b son dos elementos cualesquiera de E , los espacios homogéneos $(\mathcal{C}_a, G)$ y $(\mathcal{C}_b, G)$ son isomorfos.*

Caso particular. — De cuanto precede resulta que los conjuntos E y $\mathcal{C}_a$ ($\mathcal{C}_b, \dots$) que se corresponden biyectivamente, son finitos al mismo tiempo y tienen entonces el mismo número de elementos, igual al índice (común) de los estabilizadores $G_a, G_b, \dots$ de los diferentes elementos de E . En este caso escribiremos, indicando por n_E el número de elementos de E :

$$(12) \quad n_E = i(G_a).$$

Un caso más particular es aquel en que el grupo G es finito: entonces el subgrupo G_a es necesariamente de índice finito y se tiene:

$$(13) \quad n_E = i(G_a) = \frac{O(G)}{O(G_a)}.$$

Vemos, pues, que si un grupo G de orden finito opera transitivamente en un conjunto E , E tiene necesariamente un número finito de elementos y este número n_E es divisor del orden del grupo G .

Nota. — En las consideraciones precedentes se puede, desde luego, reemplazar el grupo de operadores dado, G , por su imagen homomorfa Γ en el grupo $\mathcal{S}(E)$ de las biyecciones de E y escribir, designando por Γ_a el estabilizador de a en Γ :

$$n_E = i(\Gamma_a)$$

o, si Γ es de orden finito,

$$n_E = i(\Gamma_a) = \frac{O(\Gamma)}{O(\Gamma_a)}.$$

Adviértase que Γ puede ser finito sin que lo sea G .

Grupo intransitivo en un conjunto E. — Cuando un grupo G opera intransitivamente en un conjunto E (por lo que se dice, simplemente, *grupo intransitivo en E*) aparecen en este E distintas clases de transitividad A_k (donde el conjunto de los subíndices lo designaremos por K) y otros tantos espacios homogéneos (A_k, G) .

Estudiemos el caso en que el conjunto E es finito y con n elementos. El conjunto K es finito, e indicando por v_k el número de elementos de A_k tendremos, según (12),

$$(14) \quad n = \sum_{k \in K} v_k = \sum_{k \in K} i(G_k)$$

donde G_k es el estabilizador en G de un elemento cualquiera a_k de A_k e $i(G_k)$ su índice en G . Si G es un grupo de orden finito, $O(G) = N$, todos los índices $i(G_k)$ son divisores (propios o impropios) del entero N .

La igualdad (14), que llamaremos *ecuación de las clases generalizadas*, tiene importantes aplicaciones.

Aplicación 1. — Consideremos un grupo finito G de orden N , $O(G) = N$, operando en sí mismo por los automorfismos internos. Cada elemento z del centro Z es una clase de transitividad, su estabilizador G_z es el propio G y tiene por índice $i(G_z) = 1$. Para otro elemento cualquiera a_k el índice $i(G_k)$ es un divisor de N mayor que 1. Si ponemos $O(Z) = \zeta$, la ecuación (14) toma la forma

$$(14') \quad N = \zeta + \sum' v_k \quad (v_k | N, v_k > 1)$$

Esta ecuación, que se llama *ecuación de las clases*, implica numerosas consecuencias. Limitémonos a señalar la siguiente: Si el orden N del grupo G es una potencia de un número primo

$$N = p^a \quad (p \text{ primo})$$

los enteros v_k que figuran tras el signo $\sum'$ son todos potencias de p de exponentes λ_k positivos y la igualdad (14') se escribe

$$p^a = \zeta + \sum' p^{\lambda_k} \quad (\lambda_k > 0)$$

de donde: *El orden del centro Z es divisible por p .*

Un grupo de orden p^a (p primo) se llama *p-primario*; podemos enunciar:

Teorema 3. — *El centro de un grupo p -primario no se reduce nunca elemento unidad.*

Corolario. — *Un grupo p -primario G de orden p^α , con α mayor que 1 y no abeliano ¹⁾ no es nunca simple.*

En efecto, el centro Z de G , subgrupo distinguido de G , es un subgrupo propio, según el teorema 3.

Aplicación 2. — Consideremos otra vez un grupo finito G de orden N . Sea p un factor primo de N y sea p^r la más alta potencia de p que divide a N :

$$N = mp^r \quad \text{con} \quad (m, p) = 1.$$

Como hemos visto, G opera por las traslaciones a la izquierda, en la familia $\mathcal{F}$ de las partes $A, \dots$ de G que tienen λ elementos.

Tomemos

$$\lambda = p^\alpha, \quad 1 \leq \alpha \leq r.$$

El conjunto $\mathcal{F}$, que ahora designaremos por $\mathcal{F}_\alpha$, queda descompuesto en clases de transitividad C_k ($k \in K$); sea G_k el estabilizador en G de una parte $A_k \in C_k$: la ecuación de las clases (14) da

$$(14'') \quad n_\alpha = \sum_{k \in K} i(G_k)$$

donde n_α es el número de elementos del conjunto considerado $\mathcal{F}_\alpha$ y $i(G_k)$ es el índice de G_k en G .

Ahora tenemos:

$$\begin{aligned} n_\alpha &= \binom{N}{p^\alpha} = \binom{mp^r}{p^\alpha} = \frac{mp^r}{p^\alpha} \cdot \frac{mp^r - 1}{1} \cdot \frac{mp^r - 2}{2} \cdot \dots \cdot \frac{mp^r - (p^\alpha - 1)}{p^\alpha - 1} \\ &= mp^{r-\alpha} \binom{mp^r - 1}{p^\alpha - 1} = mp^{r-\alpha} \nu \end{aligned}$$

donde el entero ν se expresa

$$\nu = \prod_{s=1}^{p^\alpha-1} \left(-1 + \frac{mp^r}{s} \right).$$

Ahora bien, puesto que tenemos $\alpha \leq r$ y $s \leq p^\alpha - 1$, la mayor potencia de p que puede dividir a s es menor que p^r ; cada uno de los factores del segundo

¹⁾ Si G es abeliano el corolario también es válido y significa que G , de orden p^α , $\alpha > 1$, tiene un subgrupo propio. Esto se ve notando (ver Cap. III, § 3) que, si G no es cíclico, un elemento $a \neq e$ engendra un subgrupo propio mientras que, si G es cíclico, $G = \langle a \rangle$, a engendra un subgrupo propio.

miembro es, pues, de la forma

$$-1 + \frac{mp^{r'}}{s'} \quad \text{con} \quad r' > 0 \quad \text{y} \quad (s', p) = 1$$

Dicho esto, si p es distinto de 2, luego impar, $p^\alpha - 1$ es par y, puesto que el producto de los s' es primo con p , el entero v es de la forma

$$v = 1 + hp \quad (h \text{ entero}).$$

Para $p = 2$ tenemos: $v = -1 + hp$, pero, reemplazando h por $h + 1$, también podemos escribir v en la forma precedente. Finalmente, en todo caso tenemos:

$$(15) \quad n_\alpha = mp^{r-\alpha} \cdot (1 + hp) \quad (h \text{ entero}).$$

De esta expresión de los C_k resulta que existe al menos una clase de transitividad C_k tal que el índice $i(G_k)$ correspondiente sea divisible por una potencia de p al menos igual a $p^{r-\alpha}$, lo que implica

$$O(G_k) \geq p^\alpha.$$

Pero G es el estabilizador de una parte $A_k \in C_k$ que tiene p^α elementos: esta parte es invariante para todo elemento g de G_k ($gA_k = A_k, \forall g \in G_k$); tenemos, pues,

$$ga \in A_k \quad \forall g \in G_k \quad \text{y} \quad \forall a \in A_k$$

de donde

$$G_k a \subseteq A_k$$

y por consiguiente A_k contiene la trayectoria, por G_k , de uno de sus elementos. Según la regla de simplificación, el número de elementos de esta trayectoria es el orden de G_k : tenemos entonces, puesto que A_k tiene p^α elementos,

$$O(G_k) \leq p^\alpha,$$

de donde la igualdad. De este modo,

$$G_k \text{ es un subgrupo de } G \text{ de orden } p^\alpha;$$

en consecuencia, resulta que A_k es la trayectoria por G_k de uno cualquiera de sus elementos:

$$A_k = G_k a \quad (\forall a \in A_k).$$

Pero la clase de transitividad considerada C_k , al contener a A_k , contiene todo complejo gA_k deducido de A_k por una traslación a la izquierda, en particular C_k contiene a

$$a^{-1} A_k = a^{-1} G_k a = H_a$$

que es, como G_k , un subgrupo de orden p^α . Además, todo complejo $X \in C_k$ se deduce de H_a por una traslación a la izquierda, luego es una clase a la iz-

quiera relativa a H_a . Resulta que toda clase C_k del tipo considerado [$i(G_k)$ divisible a lo más por p^{r-a}] contiene un subgrupo de orden p^a y uno solo.

Recíprocamente, está claro que para todo subgrupo de orden p^a , el conjunto de clases a la izquierda es una clase de transitividad C_k de este tipo.

Luego, si s_a es el número de subgrupos de orden p^a , la ecuación de las clases (14'') se escribe, teniendo en cuenta (15):

$$n_a = mp^{r-a}(1 + hp) = s_a mp^{r-a} + tp^{r-a+1},$$

de donde

$$m(1 - s_a) = (t - mh)p$$

y, puesto que p es primo con m :

$$s_a \equiv 1 \quad (p)$$

Con esto hemos obtenido el

Teorema 4 (primer teorema de Sylow). — *Un grupo G cuyo orden es divisible precisamente por p^r , admite, para todo entero α comprendido entre 1 y r , subgrupos de orden p^α . El número de estos subgrupos es congruente con 1 módulo p .¹⁾*

Si hacemos $\alpha = 1$ vemos, en particular, que el grupo G contiene elementos de orden p (Cauchy).

Si hacemos $\alpha = r$ obtenemos los llamados *p -subgrupos de Sylow*, que son aquellos cuyo orden es igual a la más alta potencia de p que divide al orden de G .

Sea S un p -subgrupo de Sylow de G . Las clases a la izquierda de G relativas a S tienen p^r -elementos; su conjunto $\mathcal{F}$, que tiene m elementos, es una parte de $\mathcal{F}(G)$ invariante para todo subgrupo G' de G operando por las traslaciones a la izquierda.

Tomemos para G' un subgrupo H de orden p^α ($1 \leq \alpha \leq r$). Puesto que el número m de elementos de $\mathcal{F}$ es primo con p , al menos una clase de transitividad $\mathcal{D}$ tiene un número de elementos no múltiplo de p . Ahora, este número es el índice $i(D)$ del estabilizador, en H , de un complejo $B \in \mathcal{D}$ ($\subseteq \mathcal{F}$): $i(D)$ es divisor de $O(H) = p^\alpha$, lo que exige

$$i(D) = 1.$$

La clase $B = bS$, elemento único de su clase de transitividad $\mathcal{D}$, es, pues, invariante por H (operando por las traslaciones a la izquierda),

$$HbS = bS,$$

de donde

$$HbSb^{-1} = bSb^{-1}$$

y

$$H \subseteq bSb^{-1},$$

¹⁾ Decimos que N es divisible precisamente por p^r , cuando N es múltiplo de p^r y no lo es de p^{r+1} (p , primo). (N. del T.)

puesto que bSb^{-1} es, como S , un subgrupo e incluso un p -subgrupo de Sylow.

Para $\alpha = r$ los dos subgrupos H y bSb^{-1} , del mismo orden, coinciden necesariamente. Con esto obtenemos el

Teorema 5 (segundo teorema de Sylow). — *En un grupo G cuyo orden es divisible precisamente por p^r , todo subgrupo de orden p^r está contenido en un p -subgrupo de Sylow; todos los p -subgrupos de Sylow son conjugados de uno de ellos (es decir, son sus transformados por los automorfismos internos).*

§ 7. Leyes de composición externa. Grupos con operadores

Al principio del § 6 hemos considerado un conjunto E provisto de un dominio de operadores Ω , con la ley externa $*$, y hemos estudiado el caso en que Ω tenía una ley de composición interna, denotada $\cdot$, y poseía un eventual elemento neutro ε relativo a esa ley. En el caso en que Ω sea un grupo para la ley $\cdot$, hemos visto la importancia de las dos reglas de cálculo:

$$(1) \quad (\omega_2 \cdot \omega_1) * x = \omega_2 * (\omega_1 * x) \quad (\text{asociatividad mixta}).$$

$$(2) \quad \varepsilon * x = x, \forall x \in E \quad (\varepsilon \text{ operador unidad}).$$

Nos quedan por considerar otras reglas de cálculo, importantes de por sí, que nos llevan a la noción de *grupo con operadores* (y a las nociones más particulares de módulo y de espacio vectorial, que estudiamos en el Capítulo VIII). Supondremos desde ahora el conjunto E provisto de una ley interna de composición que denotamos con τ en el caso general.

A cada elemento ω de Ω asociamos otra vez la aplicación $\varphi = \alpha(\omega)$ de E en E definida por

$$\varphi(x) = \omega * x.$$

Un caso notable es, evidentemente, aquel en el que todas estas aplicaciones φ sean *endomorfismos* de E (para la ley τ), es decir:

$$(3) \quad \varphi(x \tau y) = \varphi(x) \tau \varphi(y), \quad \forall \omega \in \Omega \quad \text{y} \quad \forall x, y \in E.$$

Si volvemos a los operadores, esta condición se escribe:

$$(3') \quad \omega * (x \tau y) = (\omega * x) \tau (\omega * y), \quad \forall \omega \in \Omega \quad \text{y} \quad \forall x, y \in E.$$

Bajo esta forma, ello significa que *la ley externa $*$ es distributiva a la izquierda para la ley interna τ del conjunto E . Ésta se llama condición de distributividad a la izquierda* (análogamente interviene la distributividad a la derecha, si se trata de una ley externa a la derecha).

Cuando esta condición se verifica, se dice que el dominio Ω de operadores (a la izquierda) es *distributivo (a la izquierda)*. Para más comodidad, vamos a designar un dominio tal por $\mathcal{A}$, y sus elementos por $\lambda, \mu, \dots$

Notaciones particulares. — Frecuentemente la ley externa se denota multiplicativamente. Si la ley interna está denotada aditivamente, la condición (3') se escribe:

$$(3'') \quad \lambda(x + y) = \lambda x + \lambda y, \quad \forall \lambda \in \Delta \quad y \quad \forall x, y \in E.$$

y, si la ley interna de E se denota multiplicativamente:

$$(3''') \quad \lambda(xy) = (\lambda x)(\lambda y) \quad \forall \lambda \in \Delta \quad y \quad \forall x, y \in E.$$

Naturalmente, si el dominio de operadores $\Delta (= \Omega)$ tiene él mismo una ley de composición interna, la distributividad a la izquierda de la ley externa $*$ respecto a la ley interna τ de E puede coexistir con la asociatividad mixta (1). Otro caso notable es aquel en que Δ tiene una ley interna *distributiva a la derecha* para la ley externa $*$, es decir, designando aquí esta ley interna de Δ por $\perp$:

$$(4) \quad (\lambda \perp \mu) * x = (\lambda * x) \tau (\mu * x), \quad \forall \lambda, \mu \in \Delta \quad y \quad \forall x \in E.$$

Esta regla de cálculo se llama *distributividad mixta a la derecha* de la ley externa respecto a la ley interna $\perp$ de Δ ; la palabra *mixta* recuerda que en el segundo miembro los dos productos externos $\lambda * x$ y $\mu * x$ se componen por la *ley interna* τ de E . No debe perderse esto de vista cuando se utilizan notaciones particulares, por ejemplo la notación multiplicativa para la ley externa y la notación aditiva para ambas leyes internas, de Δ y de E . La fórmula (4) toma entonces el aspecto familiar

$$(4') \quad (\lambda + \mu)x = \lambda x + \mu x, \quad \forall \lambda, \mu \in \Delta \quad y \quad \forall x \in E.$$

pero el signo $+$ del primer miembro indica la adición en Δ , mientras que el $+$ del segundo indica la adición en E .

Advirtamos todavía, a propósito de la fórmula (4), que si $\varphi = \alpha(\lambda)$, $\psi = \alpha(\mu)$, $\chi = \alpha(\lambda + \mu)$ son las aplicaciones (de E en E) definidas por los operadores λ , μ , $\lambda + \mu$, y si $\mathbf{T}$ designa la ley interna deducida de τ por paso a las aplicaciones o a las funciones (Cap. I, § 4, 1.º), la condición (4) se escribe

$$\chi(x) = \varphi(x) \mathbf{T} \psi(x) = (\varphi \mathbf{T} \psi)(x), \quad \forall x \in E,$$

luego

$$\chi = \varphi \mathbf{T} \psi$$

o, finalmente,

$$\alpha(\lambda \perp \mu) = \alpha(\lambda) \mathbf{T} \alpha(\mu).$$

Por consiguiente, la familia Φ de las aplicaciones $\alpha(\lambda)$, $\lambda \in \Delta$, es estable para la ley $\mathbf{T}$ y α es un *homomorfismo* que aplica Δ , con ley de composición $\perp$, sobre Φ , con la ley $\mathbf{T}$.

Examinemos algunos casos particulares y algunos ejemplos.

Definición. — Un grupo G al que se asigna un dominio de operadores Δ distributivo respecto a la ley interna de G , se llama *grupo con operadores*. Se dice entonces, de modo abreviado y cómodo, que G es un Δ -grupo. Insistamos en que estas expresiones implican la validez de las fórmulas distributivas (3), (3'), (3'') y (3'''), según las notaciones utilizadas.

Ejemplo 1 a. — A un grupo G cualquiera asociemos, como único operador, la aplicación idéntica ε de G sobre sí mismo:

$$(2) \quad \varepsilon * x = \varepsilon(x) = x \quad \forall x \in G.$$

Asignándole este dominio $\Delta = \{\varepsilon\}$ (en el cual $\varepsilon^2 = \varepsilon \circ \varepsilon = \varepsilon$), G es un grupo con operadores, en el que la distributividad a la izquierda (3) o (3''') se satisface evidentemente. Además, con (2) tenemos la asociatividad mixta (1).

Ejemplo 1 b. — Un grupo G cualquiera opera en sí mismo por los automorfismos internos

$$s * x = sxs^{-1}$$

cumpléndose las condiciones (1) y (2) (§ 6). Como los automorfismos internos son endomorfismos particulares [cfr. § 5; $s*(xy) = sxy s^{-1} = sxs^{-1} \cdot sys^{-1} = (s*x)(s*y)$], se verifica la condición (3).

Ejemplo 1 c. — Reduciendo el anterior dominio de operadores $\Delta = G$, nos vemos conducidos a asignar a G un dominio de operadores Γ constituido por los *automorfismos internos* ($\Gamma \simeq G/Z$). Las condiciones (1), (2) y (3) siguen cumpliéndose.

Ejemplo 1 d — Más generalmente, se hace de un grupo cualquiera un grupo con operadores asignándole un dominio distributivo Δ que sea una familia cualquiera de endomorfismos de G . Son particularmente importantes, con el grupo Γ de los automorfismos internos, el semigrupo Δ_1 de todos los *endomorfismos de G* y el grupo Δ_2 de todos los automorfismos de G .

Ejemplo 2. — Consideremos un *grupo abeliano* G con notación aditiva; recordemos que, para todo entero $\lambda \geq 0$, λx designa el elemento neutro 0 de G si $\lambda = 0$, la suma de λ elementos iguales a x si $\lambda > 0$, la suma de λ elementos iguales a $-x$ si $\lambda < 0$ (cfr. Cap. II, § 2). Tenemos así una ley de composición externa que aplica el producto $\mathbf{Z} \times G$ en G y que cumple las condiciones (1) (para la multiplicación en $\mathbf{Z}$), (2), (3'') y (4').

Veremos en el Capítulo VIII que estas condiciones se expresan con decir que todo grupo abeliano G es un $\mathbf{Z}$ -módulo unitario. Por ejemplo, $\mathbf{Z}$ considerado como grupo aditivo, es él mismo un $\mathbf{Z}$ -módulo unitario. El subconjunto M de los múltiplos de un entero fijo m (≥ 0), subgrupo aditivo de $\mathbf{Z}$, es él mismo un $\mathbf{Z}$ -módulo unitario. El conjunto V de los vectores libres de coordenadas reales

en el espacio de tres dimensiones, $\mathbf{R}^3$, considerado como grupo abeliano respecto a la adición geométrica, es un $\mathbf{R}$ -módulo unitario. En este último caso, la propiedad suplementaria de que la división por todo número distinto de 0 resulta posible, implica nuevas propiedades, que expresaremos diciendo que V es un *espacio vectorial* sobre $\mathbf{R}$.

Terminaremos por una propiedad con frecuencia útil. Dados un conjunto E con un dominio de operadores Ω y la ley externa correspondiente que denotaremos multiplicativamente, una relación de equivalencia $\mathcal{R}$ definida en E se llama Ω -*equivalencia* (o bien se dice que es *licita*, o *compatible*, para la ley externa) si

$$a \equiv b(\mathcal{R}) \quad \text{implica} \quad \omega a \equiv \omega b(\mathcal{R}) \quad \forall \omega \in \Omega.$$

El interés de esta propiedad estriba en que permite definir el producto ωA , donde A es una clase módulo $\mathcal{R}$, como la clase P que contiene uno cualquiera de los productos ωa , donde a es un elemento de E perteneciente a la clase A (esta clase P es efectivamente independiente de la elección de a en A). Entonces Ω es también un dominio de operadores para el conjunto cociente $E/\mathcal{R}$. Establecido esto, tenemos las siguientes propiedades.

Supongamos primero el *conjunto E provisto de una ley de composición interna*, que denotaremos multiplicativamente, y $\mathcal{R}$ compatible con esa ley: esto permite definir del modo usual una multiplicación en $E/\mathcal{R}$. Si la *condición distributiva (3''')* se cumple en E , también se cumple en $E/\mathcal{R}$. En efecto, dadas dos clases cualesquiera X, Y , y dos elementos, x de X e y de Y , la clase $\omega(XY)$ es la que contiene al elemento $\omega(xy) = \omega(x)\omega(y)$, la cual pertenece a la clase $(\omega X)(\omega Y)$; resulta por tanto

$$\omega(XY) = (\omega X)(\omega Y).$$

Asimismo resulta que dado un grupo con operadores G (provisto de un dominio distributivo Δ) el grupo cociente $G/\mathcal{R}$, donde $\mathcal{R}$ es una Δ -equivalencia compatible, es también un Δ -grupo.

De modo análogo, consideremos de nuevo un conjunto E cualquiera y supongamos el dominio de operadores Ω provisto de una ley interna denotada multiplicativamente. Si $\mathcal{R}$ es una Ω -equivalencia, y si la *condición de asociatividad mixta (1)* se cumple en E , también se cumple en $E/\mathcal{R}$. En efecto, si es $x \in X$, entonces $(\omega_1\omega_2)X$ es la clase que contiene al elemento $(\omega_1\omega_2)x = \omega_1(\omega_2x)$; ahora, ω_2x está en la clase ω_2X y $\omega_1(\omega_2x)$ en la clase $\omega_1(\omega_2X)$; tenemos, pues,

$$(\omega_1\omega_2)X = \omega_1(\omega_2X).$$

Si, además, Ω admite un elemento neutro ϵ , operador-unidad para E , es claro que también ϵ es operador unidad para $E/\mathcal{R}$.

Asimismo resulta que si un grupo Ω opera en E , opera también en el conjunto cociente $E/\mathcal{R}$, cuando $\mathcal{R}$ es una Ω -equivalencia.

CAPÍTULO III

GENERACIÓN DE GRUPOS

§ 1. Sistemas de generadores; conmutadores. Unión completa

Consideremos un grupo G y la familia de Moore $\mathcal{S}$ constituida por los subgrupos de G (cap. II, § 4); a $\mathcal{S}$ corresponde una clausura de Moore,

$$M \rightarrow \bar{M}$$

que a una parte no vacía M de G asocia la intersección $\bar{M}$ de todos los subgrupos que contienen a M ; $\bar{M}$ es un subgrupo ($\bar{M} \in \mathcal{S}$), y precisamente *el menor subgrupo de G que contiene a M* (cap. I, § 4, 5.º): se dice entonces que $\bar{M}$ es *el subgrupo engendrado por M* y también que M es *un sistema de generadores para $\bar{M}$* .

Cualquier subgrupo H que contenga a M , en particular $\bar{M}$, contiene también a todo producto cuyos factores, en número finito, sean elementos de M o inversos de elementos de M . Sea $\tilde{M}$ el conjunto de tales productos: Tendremos $\tilde{M} \subseteq \bar{M}$. Pero $\tilde{M}$ es un subgrupo de G , pues si p, p_1 son dos productos formados con los elementos de M o de M^{-1} , pp_1^{-1} es también un producto de ese tipo; por otra parte $\tilde{M}$ contiene a M (pues $m \in M$, implica $m = mm^{-1}m \in \tilde{M}$): es decir, $\bar{M} \subseteq \tilde{M}$. En consecuencia $\bar{M} = \tilde{M}$. Enunciemos:

Teorema 1. — *El subgrupo $\bar{M}$ engendrado por una parte no vacía M de un grupo G es el conjunto de los productos con un número finito de factores que son elementos de M o inversos de elementos de M .*

De este modo, cualquier elemento x de $\bar{M}$, tiene al menos una representación de la forma

$$x = m_{i_1}^{\alpha_1} \dots m_{i_p}^{\alpha_p}, \quad \text{donde } m_{i_\lambda} \in M, \quad \alpha_\lambda \in \mathbb{Z}.$$

Un mismo grupo admite generalmente sistemas diferentes de generadores. Por ejemplo, si el grupo G no se reduce a su elemento unidad e , $G \neq \{e\}$, admite como sistema de generadores G y $G - \{e\}$. El grupo *aditivo* $\mathbb{Z}$ de los enteros

de cualquier signo admite como sistema de generadores $\{1\}, \{-1\}, \{n, n+1\}$ $\forall n \in \mathbb{Z}$, $N = \{1, 2, \dots, n, \dots\}$.

Llamamos *sistema irreducible* o *sistema minimal* de generadores de un grupo G un sistema de generadores M tal que ninguna parte propia M' de M sea un sistema de generadores de G ; tal sistema irreducible está, pues, caracterizado así:

$\overline{M} = G$ y $M' \subset M$ (estrictamente) implican $\overline{M'} \subset \overline{M} = G$ (estrictamente).

Por ejemplo, para el grupo aditivo $\mathbb{Z}$, los sistemas de generadores $\{1\}$, $\{-1\}$, $\{n, n+1\}$ para $n \notin \{-2, -1, 0, 1\}$ son irreducibles; el sistema $\{n, n+1\}$ para $n \in \{-2, -1, 0, 1\}$ no es irreducible; el sistema N tampoco lo es.

Veamos otro ejemplo importante de subgrupo definido por un sistema de generadores. El *conmutador* de dos elementos x, y de un grupo G es, por definición, el elemento

$$xyx^{-1}y^{-1}.$$

Se llama *grupo conmutador* (o *grupo derivado* o *primer derivado*) de G el subgrupo C engendrado por el conjunto de los conmutadores. El inverso del conmutador $xyx^{-1}y^{-1}$ es $yxy^{-1}x^{-1}$, es decir un conmutador, de modo que C sea simplemente el conjunto de todos los productos de un número finito de conmutadores.

Para que G sea abeliano, es necesario y suficiente que se tenga $C = (e)$.

Teorema 2. — *Cualquier subgrupo H que contenga al grupo conmutador C (como, en particular, el propio C), es subgrupo distinguido de G .*

Sea $h \in H$, $x \in G$, tenemos

$$xhx^{-1} = xhx^{-1}h^{-1}h \in H$$

puesto que $xhx^{-1}h^{-1} \in C \subseteq H$.

Teorema 3. — *Para que el grupo cociente G/H de G por un subgrupo distinguido H sea abeliano, es necesario y suficiente que H contenga el grupo conmutador C .*

Sean $X = xH$, $Y = yH$ dos clases cualesquiera relativas a H , que contienen respectivamente los elementos x, y de G . La clase $XYX^{-1}Y^{-1}$ es la que contiene el elemento $xyx^{-1}y^{-1}$. Para que coincida con la clase H , elemento unidad de G/H , es necesario y suficiente que el conmutador $xyx^{-1}y^{-1}$ pertenezca a H . Luego, para que G/H sea abeliano, es necesario y suficiente que el subgrupo H de G contenga al conjunto de conmutadores, y por consiguiente al grupo C engendrado por este conjunto.

En particular, el grupo cociente G/C es abeliano. El paso de G a su imagen homomorfa abeliana G/C se llama la *abelización* de G .

Consideremos ahora una familia $\mathcal{F}$ (finita o infinita) de subgrupos de un grupo G , $\mathcal{F} \subseteq \mathcal{S}$ ($\mathcal{S}$ designa siempre la familia de Moore de todos los subgrupos de G). A esta familia $\mathcal{F}$ está asociada en principio la *intersección con-*

juntista de subgrupos que pertenecen a $\mathcal{F}$: esta intersección $I = \bigcap_{S \in \mathcal{F}} S$ es el

mayor subgrupo contenido en todos y cada uno de los subgrupos $S \in \mathcal{F}$.

Existe igualmente un subgrupo mínimo de G que contiene a todo subgrupo $S \in \mathcal{F}$ es evidentemente el subgrupo C engendrado por la unión conjuntista $R = \bigcup_{S \in \mathcal{F}} S$ de los subgrupos que pertenecen a $\mathcal{F}$:

$$C = \overline{R} = \overline{\bigcup_{S \in \mathcal{F}} S}.$$

El grupo C así definido, se llama *unión completa* de los subgrupos S ; también se dice que es el *supremo* de $\mathcal{F}$ en la familia S de los subgrupos de G .

El teorema 1 nos da otra definición. Puesto que R es una unión de subgrupos, el inverso de cualquier elemento de R es un elemento de R ; en consecuencia la unión completa C es el conjunto de los productos c de un número finito variable, k , de factores tomados en R , es decir en los grupos S_i que pertenecen a la familia $\mathcal{F}$:

$$c = s_1 \dots s_k, \quad s_i \in S_i, \quad S_i \in \mathcal{F}$$

(los S_i no son necesariamente distintos). En general, la unión completa R es distinta de la unión conjuntista R de los subgrupos de $\mathcal{F}$. Un caso importante en que $\overline{R} = R$ es el caso en que $\mathcal{F}$ es una *cadena*, es decir, cuando entre dos subgrupos cualesquiera de $\mathcal{F}$ uno contiene al otro. En este caso R es un subgrupo, ya que r_1 y $r_2 \in R$ significa $r_i \in S_i, S_i \in \mathcal{F}$ ($i = 1, 2$); luego, si S es aquel subgrupo S_1 o S_2 que contiene al otro, r_1 y $r_2 \in S$, luego $r_1 r_2 \in S \subseteq R$, luego R es un subgrupo, lo que evidentemente implica $\overline{R} = R$.

Si los subgrupos S de la familia $\mathcal{F}$ son *permutables dos a dos*

$$SS' = S'S \quad \forall S, S' \in \mathcal{F},$$

en particular si $\mathcal{F}$ es una *familia de subgrupos distinguidos* como sucede siempre que G sea un *grupo abeliano*, se puede escribir cada elemento c de C de manera que contenga a lo más un factor que pertenece a cada grupo S de la familia $\mathcal{F}$. C toma entonces el nombre de *producto* de los grupos de esta familia, si G está escrito multiplicativamente, o de *suma* de los grupos de esta familia, si G está escrito aditivamente. Es claro que si la familia $\mathcal{F}$ es finita, ese producto coincide con el producto en el conjunto de las partes $\mathfrak{P}(G)$, en el sentido ya definido (cap. I, § 4).

El producto C de una familia $\mathcal{F}$ de subgrupos distinguidos de un grupo G es un subgrupo distinguido. Sea en efecto

$$c = s_1 s_2 \dots s_k, \quad s_i \in S_i, \quad S_i \in \mathcal{F}$$

un elemento de C ; para todo elemento x de G , tenemos

Señalemos en fin que, en un grupo abeliano G con notación aditiva, por ejemplo, el subgrupo engendrado por un conjunto finito $M = \{m_1, \dots, m_r\}$ es la suma de los r subgrupos engendrados por cada uno de los elementos m_i .

§ 2. Grupo simétrico

Nos proponemos estudiar el grupo simétrico S_n , es decir el grupo de las permutaciones del conjunto $E_n = \{1, 2, \dots, n\}$; mostremos al principio explícitamente algunos sistemas notables de generadores de ese grupo.

Para simplificar la escritura, indicaremos la composición de las permutaciones, con notación multiplicativa en vez de usar símbolo $\circ$.

Se llama *trasposición*, en S_n , a una permutación que cambie sólo dos elementos;

$$\tau_{ij} = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

cualquier trasposición $\tau_{ij} (= \tau_{ji})$, es un elemento involutivo:

$$\tau_{ij}^2 = e$$

y engendra un subgrupo de orden 2. El número de trasposiciones es el de pares (i, j) no ordenados, es decir, sin hacer distinción entre el par (i, j) y el par (j, i) , número igual a $\frac{1}{2}n(n-1)$. Esto se ve también observando que obtenemos todas las trasposiciones permutando cada uno de los elementos $1, 2, \dots, n$ con cada uno de los que le siguen (en el orden natural); el número de trasposiciones es por consiguiente

$$n-1 + n-2 + \dots + 1 = \frac{1}{2}n(n-1).$$

Teorema 1. — *El conjunto de trasposiciones es un sistema de generadores para el grupo simétrico S_n .*

El teorema es evidente para $n=2$; razonemos por recurrencia para n . Sea α una permutación de S_n .

Si $\alpha(n) = n$, la restricción de α al conjunto $E_{n-1} = \{1, 2, \dots, n-1\}$ es una permutación $\alpha' \in S_{n-1}$, que es el producto π' de trasposiciones $\tau' \in S_{n-1}$.

Pero poniendo

$$\begin{aligned} \tau(x) &= \tau'(x) & \text{para } x \in E_{n-1} \\ \tau(n) &= n \end{aligned}$$

queda definida una trasposición $\tau \in \mathcal{S}_n$, para cada una de las trasposiciones $\tau' \in \mathcal{S}_{n-1}$, y α es igual al producto π de esas trasposiciones τ (ya que α y π dejan fijo el elemento n y tienen la misma restricción, $\alpha' = \pi'$ a E_{n-1}).

Si $\alpha(n) = n' < n$, la permutación $\tau_{nn'}\alpha = \beta$ deja a n invariante, luego (primer caso) es un producto de trasposiciones, y entonces sucede lo mismo con $\alpha = \tau_{nn'}\beta$.

El conjunto de las $\frac{1}{2}n(n-1)$ trasposiciones posibles constituyen, pues, un sistema de generadores para $\mathcal{S}_n$. Ese sistema, para $n > 2$, no es irreducible, como demuestra la proposición siguiente:

Teorema 2. — *Las $n-1$ trasposiciones $(1, 2), (2, 3), \dots, (n-1, n)$ constituyen, para $\mathcal{S}_n$, un sistema de generadores irreducible Σ .*

Para trasponer i y j (con $i < j$ por ejemplo), se puede cambiar sucesivamente i con $i+1$, $i+1$ con $i+2$, ..., $j-1$ con j , $j-1$ con $j-2$, ..., $i+1$ con i ; tendremos la igualdad:

$$(i, j) = (i, i+1) \dots (j-2, j-1) (j-1, j) \dots (i+1, i+2) (i, i+1)$$

El segundo miembro es el producto de $2(j-i)-1$ trasposiciones del sistema Σ mientras (i, j) es una trasposición cualquiera. Luego por el teorema 1, Σ es un sistema de generadores.

Este sistema es irreducible, pues si se quita de Σ la trasposición $(i, i+1)$ se obtiene un sistema Σ' que engendra un subgrupo H cuyas permutaciones cambian entre sí los elementos $1, \dots, i$ y también entre sí los elementos $i+1, \dots, n$: H es, pues, un subgrupo propio de $\mathcal{S}_n$.

Corolario. — *El grupo simétrico $\mathcal{S}_n$ se engendra por la trasposición:*

$$\tau = (1, 2)$$

y la permutación circular

$$\gamma = (1, 2, \dots, n) \quad \text{ó} \quad \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix},$$

Tenemos, en efecto,

$$\gamma^k = \begin{pmatrix} 1 & 2 & \dots & n-k & n-k+1 & \dots & n \\ k+1 & k+2 & \dots & n & 1 & \dots & k \end{pmatrix}$$

y

$$\gamma^k \tau \gamma^{-k} = (k+1, k+2)$$

Así, pues, las $n - 1$ trasposiciones del sistema Σ pertenecen al subgrupo K engendrado por τ y γ ; según el teorema 2, resulta $K = S_n$.

Observación. — Para $n > 2$, τ y γ son distintos y forman un *sistema irreducible de dos generadores*. Vemos así que los diferentes sistemas irreducibles de generadores de un mismo grupo no tienen necesariamente el mismo número de elementos.

Señalemos también que la representación de una permutación como producto de trasposiciones (cualesquiera, o tomadas en el sistema Σ), no es única, y así por ejemplo, suponiendo $n \geq 4$,

$$(1, 2) = (3, 4) (1, 2) (3, 4)$$

Pero vamos a ver que todas esas representaciones de una permutación dada, tienen de común una propiedad interesante: *la paridad del número de trasposiciones*; ya hemos constatado antes, en este orden de ideas, que la trasposición (i, j) es el producto de un número *impar*, $2(j - i) - 1$, de trasposiciones de Σ .

Atribuyamos a una permutación α el número ν_α de las *inversiones* de esta permutación, es decir, el número de pares (no ordenados) (i, j) tales que sea

$$\frac{\alpha(i) - \alpha(j)}{i - j} < 0,$$

consideremos luego la *paridad de ese número*, y finalmente, el número

$$\epsilon_\alpha = (-1)^{\nu_\alpha} = \pm 1,$$

llamado *signatura* de α .

Diremos que la permutación α es *par* o *impar* según que sea par o impar el número ν_α de sus inversiones, o, en forma equivalente, según que su signatura ϵ_α sea $+1$ ó -1 .

Puesto que α es una aplicación biyectiva del conjunto $\{1, 2, \dots, n\}$ sobre sí mismo, el producto

$$P_\alpha = \prod \frac{\alpha(i) - \alpha(j)}{i - j}$$

extendido a los $\frac{1}{2}n(n - 1)$ pares no ordenados (i, j) es igual a $+1$ o a -1 , y su signo es precisamente $(-1)^{\nu_\alpha}$, luego

$$P_\alpha = \epsilon_\alpha.$$

P_α es independiente del orden en el que escribimos los pares (i, j) y en consecuencia tenemos, designando por σ una permutación cualquiera:

$$\epsilon_\alpha = \prod \frac{\alpha[\sigma(i)] - \alpha[\sigma(j)]}{\sigma(i) - \sigma(j)} = \prod \frac{\alpha\sigma(i) - \alpha\sigma(j)}{\sigma(i) - \sigma(j)}$$

donde el producto se extiende siempre a los $\frac{1}{2}n(n-1)$ pares (i, j) .

De esta fórmula se deduce

$$\epsilon_\alpha \epsilon_\sigma = \prod \frac{\alpha\sigma(i) - \alpha\sigma(j)}{\sigma(i) - \sigma(j)} \cdot \prod \frac{\sigma(i) - \sigma(j)}{i - j} = \prod \frac{\alpha\sigma(i) - \alpha\sigma(j)}{i - j} = \epsilon_{\alpha\sigma}.$$

Teorema 3. — *La signatura de un producto de permutaciones es el producto de las signaturas.*

El producto de dos permutaciones pares o de dos permutaciones impares es una permutación par; el producto de una permutación par por una impar es una permutación impar.

La permutación idéntica es par; en el conjunto $E = \{1, 2, \dots, n\}$ ordenado por orden natural, una trasposición $(i, i+1)$ que cambie dos elementos consecutivos tiene evidentemente una sola inversión, luego es impar. Por consiguiente, cualquier trasposición es impar y según el teorema 2, *una permutación par es siempre el producto de un número par de trasposiciones, como una permutación impar es producto de un número impar de trasposiciones*: está, pues, bien determinada la paridad del número de factores en la expresión de una permutación como producto de trasposiciones.

Volvamos al teorema 3: significa que la aplicación

$$\alpha \rightarrow \epsilon_\alpha$$

del grupo simétrico $\mathcal{S}_n$ sobre el grupo multiplicativo $C_2 = (+1, -1) = (-1)$, grupo cíclico de orden 2, es un *homomorfismo* h . El núcleo de ese homomorfismo es el conjunto $\mathcal{A}_n$ de las permutaciones pares: este conjunto es, pues, un subgrupo distinguido de $\mathcal{S}_n$, llamado grupo alternado. Su orden es $\frac{1}{2}n!$

Determinemos el centro Z del grupo simétrico $\mathcal{S}_n$. Para $n=2$, $\mathcal{S}_n$ es de orden 2, luego es cíclico y abeliano: $\mathcal{S}_2$ coincide con su centro.

Teorema 4. — *Para $n>2$, el centro de $\mathcal{S}_n$ se reduce a la permutación idéntica. Sea ζ una permutación del centro de $\mathcal{S}_n$; tendremos la igualdad:*

$$\zeta(i, j) = (i, j)\zeta$$

(por lo demás, si esa igualdad es válida para las $n-1$ trasposiciones del sistema de generadores Σ , ζ pertenecerá al centro). Designemos por α el primer

miembro, por β el segundo; para todo índice $x \neq i, j$, tenemos $\alpha x = \zeta x$, y en consecuencia la igualdad (1) exige $\beta x = \zeta x$, de suerte que la trasposición (i, j) debe dejar ζx invariante, lo que exige que $\zeta x \neq i, j$. Así ζ debe aplicar el complementario del conjunto $\{i, j\}$ sobre sí mismo, luego puesto que ζ es una aplicación biyectiva, ζ aplica $\{i, j\}$ sobre sí mismo.

Para $n > 2$, consideremos un índice $k \neq i$; ζ debe también aplicar $\{i, k\}$ sobre sí mismo, lo que exige que $\zeta(i) = i$ ($i = 1, 2, \dots, n$).

Observación. — Volvamos al homomorfismo

$$S_n \sim C_2 = (+1, -1)$$

cuyo núcleo es el grupo alternado A_n . Para $n > 2$, el centro Z de S_n , $Z = (e)$, tiene como imagen (1), mientras que el centro de C_2 es el mismo C_2 : así, *en un homomorfismo, la imagen del centro está contenida en el centro de la imagen y la inclusión, en general, es estricta.*

En el estudio del grupo simétrico S_n , es a menudo útil, una descomposición factorial menos fina que los productos de trasposiciones, y con este fin introducimos el concepto de ciclo.

Definición. — Se llama *ciclo de longitud k* una permutación que sustituye circularmente a k elementos del conjunto $E_n = \{1, 2, \dots, n\}$ y deja invariantes a los otros $n - k$:

$$\gamma = \begin{pmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k & a_{k+1} & \dots & a_n \\ a_2 & a_3 & \dots & a_k & a_1 & a_{k+1} & \dots & a_n \end{pmatrix}$$

se escribe más simplemente así:

$$\gamma = (a_1, a_2, \dots, a_k)$$

Un ciclo de longitud k engendra un subgrupo cíclico de orden k ; es, pues, una permutación de orden k , igual al producto de $k - 1$ trasposiciones: $\gamma = (a_1, a_2) \dots (a_{k-1}, a_k)$; su signatura es $(-1)^{k-1}$.

Cualquier permutación α del grupo simétrico puede expresarse como un producto de ciclos disjuntos. Para obtener esta factorización cabe utilizar las nociones siguientes:

Indicamos por (α) el grupo cíclico engendrado por α . Llamaremos equiva-

lencia y clases de transitividad según α a la equivalencia $\mathfrak{C}$ y clases de transitividad $A, B, \dots$ según (α) . Entonces:

$$a_i \equiv a_j(\mathfrak{C}) \quad \text{significa} \quad \exists \lambda \quad \text{tal que} \quad \alpha^\lambda(a_i) = a_j,$$

luego, cada clase de transitividad A es el conjunto de transformados de un elemento a_1 de A por las potencias sucesivas de α . Pongamos:

$$\alpha(a_1) = a_2, \quad \alpha(a_2) = a_3, \dots$$

El número k de los elementos distintos así obtenidos definido por

$$\alpha(a_{k-1}) = a_k, \quad \alpha(a_k) = a_1$$

es el número de elementos de A , u *orden* de A , y la restricción de α a A es el ciclo $\gamma_A = (a_1, a_2, \dots, a_k)$, trayectoria de a_1 . Tenemos, por otra parte, $k = 1$ si α deja a a_1 invariante, y sólo en ese caso.

Así la restricción de una permutación α a una cualquiera de sus clases de transitividad, A , de orden k es un ciclo γ_A de orden k . Como las clases de transitividad de E_n son dos a dos disjuntas, dos cualesquiera de los ciclos γ_A, γ_B así obtenidos son permutables, $\gamma_A \gamma_B = \gamma_B \gamma_A$, y su producto es la restricción de α a la reunión $A \cup B$. En fin, la permutación α es el producto de los ciclos $\gamma_A, \gamma_B, \dots, \gamma_L$ correspondientes a sus diferentes clases de transitividad:

$$\alpha = \gamma_A \gamma_B \dots \gamma_L$$

(No se suele hacer figurar en el segundo miembro los ciclos de orden 1, iguales a la identidad.)

Ejemplo. — La permutación

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 2 & 7 & 1 & 6 & 9 & 3 & 4 \end{pmatrix}$$

admite la descomposición

$$\alpha = (1, 8, 3, 2, 5) (4, 7, 9) (6)$$

Un ciclo de orden k tiene por *signatura* $(-1)^{k-1}$, luego la permutación α tiene

por signatura $\epsilon_\alpha = (-1)^{\Sigma(k-1)}$; llamando r el número total de ciclos (comprendidos los de orden 1), resulta, puesto que $\Sigma k = n$:

$$\epsilon_\alpha = (-1)^{n-r}$$

podemos pues, enunciar:

Teorema 5. — *Si una permutación α de S_n es el producto de r ciclos disjuntos, para cualquier representación de α en producto de trasposiciones, el número de trasposiciones tiene la paridad de $n - r$.*

§ 3. Grupos monógenos. Grupos cíclicos

En un grupo G cualquiera, el conjunto $\{a\}$ formado por un solo elemento a , es evidentemente, un sistema de generadores *irreducible* para el subgrupo $H = \{a\}$ que él engendra. Ese subgrupo H , se llama *subgrupo monógeno engendrado por a* ; se le designa por (a) . Es un subgrupo *abeliano* de G puesto que

$$a^\lambda a^\mu = a^{\lambda+\mu} = a^\mu a^\lambda.$$

El elemento a y su inverso engendran el mismo subgrupo monógeno.

Un grupo que coincide con uno de sus subgrupos monógenos se llama *grupo monógeno*.

En el estudio de un subgrupo o de un grupo monógeno (a) , hay que distinguir dos casos

Primer caso: Las potencias a^λ del generador a son todas distintas, es decir

$$a^\lambda = a^\mu \quad \text{exige} \quad \lambda = \mu.$$

Decimos entonces que a es de orden infinito, que el grupo (a) es un grupo monógeno infinito.

Por ejemplo, el grupo aditivo de los enteros

$$\mathbf{Z} = \{ \dots, -m, \dots, -1, 0, 1, \dots, n, \dots \}$$

es un grupo monógeno infinito, que admite como generador $+1$ y -1 .

La aplicación

$$a^\lambda \rightarrow b^\lambda$$

de un grupo monógeno infinito (a) en otro grupo monógeno infinito (b), escritos ambos en forma multiplicativa, es un isomorfismo: *Dos grupos monógenos infinitos son isomorfos*. En particular, *cualquier grupo monógeno infinito es isomorfo con el grupo aditivo $\mathbf{Z}$ de los enteros relativos*.

Segundo caso: Existe al menos un par de enteros λ, μ tales que:

$$a^\lambda = a^\mu, \quad \lambda \neq \mu,$$

lo que lleva inmediatamente a la igualdad:

$$(1) \quad a^h = e, \quad h > 0$$

Sea n el menor valor de h para el que se verifica la igualdad (1)

$$(1') \quad a^n = e \quad \text{con} \quad a^m \neq e \quad \text{para} \quad 0 < m < n.$$

Por definición, n es el *orden del elemento a* ; los elementos $e, a, \dots, a^{n-1}$ son distintos y cada elemento a^λ del grupo (a) es igual a uno de ellos; en efecto, si $\lambda = qn + r$, $0 \leq r < n$, tendremos:

$$(2) \quad a^\lambda = (a^n)^q a^r = a^r.$$

Por consiguiente, el entero n es también el orden del grupo (a) (esto es, el número de sus elementos) y tal grupo se llama *cíclico de orden n* .

Por ejemplo, el grupo C_n de las permutaciones circulares (§ 4)

$$\sigma_k = \begin{pmatrix} 1 & 2 & \dots & n-k & n-k+1 & \dots & n \\ k+1 & k+2 & \dots & n & 1 & \dots & k \end{pmatrix}$$

($k = 0, 1, \dots, n-1$) es cíclico de orden n , con el generador $a = \sigma_1$. El grupo aditivo de los enteros módulo n , $\mathbf{Z}/(n)$, también es cíclico de orden n . Sea R la clase módulo n en que está el número r ($0 \leq r \leq n-1$); la aplicación biyectiva

$$a^r \rightarrow R$$

de un grupo cíclico de orden n , (a), sobre $\mathbf{Z}/(n)$ respecto a la multiplicación del grupo (a) y la adición de $\mathbf{Z}/(n)$ es un isomorfismo:

Cualquier grupo cíclico de orden n es isomorfo al grupo aditivo de los enteros módulo n .

Como se vio en el cap. II (§ 5, corolario del teorema 11), un grupo G de orden primo p no admite subgrupo propio. Por consiguiente, si a es un elemento de G , distinto de e , el subgrupo cíclico (a) coincide con G :

Todo grupo de orden primo es cíclico y, por consiguiente, abeliano.

El elemento neutro e de un grupo G es de orden 1 y es el único elemento de G que tiene esta propiedad. Un grupo G en el que todos los elementos distintos de e son de orden infinito, se llama *grupo sin torsión*; un grupo en el que todo elemento sea de orden finito se llama *periódico* o también *grupo con torsión*.

Teorema 1. — *En un grupo G , toda parte estable S cuyos elementos sean de orden finito es un subgrupo de G .*

En efecto, ya que si el elemento s de S tiene orden finito, n , su inverso es s^{n-1} , y pertenece a la misma parte estable S .

Lema. — *Sea S un subgrupo de un grupo monógeno $G = (a)$; supongamos que existe un entero positivo mínimo m tal que $a^m \in S$. Si $x = a^\lambda \in S$, debe ser $\lambda = qm$.*

Dividamos λ por m :

$$\lambda = qm + r, \text{ con } 0 \leq r < m, \quad q \in \mathbb{Z}.$$

Tendremos:

$$a^r = a^\lambda (a^{qm})^{-1} \in S$$

lo que exige $r = 0$, $\lambda = qm$, c.q.d.

Teorema 2. — *Si $G = (a)$ es un grupo cíclico de orden n , la igualdad $a^\lambda = e$ tiene lugar si $\lambda = qn$ y sólo en este caso.*

Es claro que $a^{qn} = e$. Inversamente, si $a^\lambda = e$, debe ser $\lambda = qn$ según el lema precedente, donde tomamos $S = (e)$, $m = n$.

Teorema 3. — *Cualquier subgrupo S de un grupo monógeno $G = (a)$ es monógeno.*

$E = (e)$ es, en efecto, un subgrupo monógeno, supongamos, pues, $S \neq E$. Si $a^{-\mu} \in S$, su inverso a^μ pertenece también a S y existe por consiguiente un mínimo entero positivo m tal que $a^m \in S$, de donde $(a^m) \subseteq S$. Según el lema es $S \subseteq (a^m)$, luego en definitiva $S = (a^m)$ es monógeno, c.q.d.

Consideremos ahora un grupo cíclico de orden n : $G = (a)$, $a^n = e$ ($a^\lambda \neq e$ para $\lambda = 1, \dots, n-1$).

Teorema 4. — *El subgrupo (a^k) , $1 \leq k \leq n$, engendrado por un elemento cualquiera a^k de G coincide con el subgrupo (a^d) , siendo d el máximo común divisor de k y n .*

Poniendo $n = n'd$, $k = k'd$, tendremos inmediatamente:

$$a^k = a^{k'd} \in (a^d) \quad \text{luego} \quad (a^k) \subseteq (a^d)$$

por otra parte, la relación de Bezout $d = \alpha n + \beta k$ ($\alpha, \beta \in \mathbf{Z}$), permite escribir:

$$a^d = a^{\alpha n + \beta k} = a^{\beta k} \in (a^k)$$

de donde

$$(a^d) \subseteq (a^k) \quad \text{y} \quad (a^d) = (a^k).$$

Corolario 1. — *El orden del subgrupo (a^k) es:*

$$(3) \quad n' = \frac{n}{\text{m.c.d.}(n, k)}$$

Este orden es en efecto el de (a^d) ; ahora, como d divide a n , orden de a , el orden de a^d es evidentemente $n' = n/d$: Constatamos así, en este caso particular, que el orden n' de un subgrupo del grupo cíclico G es divisor del orden n del grupo.

Corolario 2. — *Para que $x = a^k$ sea un generador del grupo cíclico $G = (a)$ de orden n , es necesario y suficiente que k y el orden n sean primos entre sí.*

El subgrupo (a^k) coincidirá con el grupo G si, y sólo si, tiene el mismo orden; y para que sea $n' = n$, es necesario y suficiente, según (3), que k y n sean primos entre sí.

Este corolario permite enunciar:

Teorema 5. — *El número de generadores distintos del grupo cíclico de orden n es igual al número $\varphi(n)$ de los enteros (positivos) primos con n y no mayores que él; $\varphi(n)$ se llama función de Euler (o indicador) del número n .*

Así tenemos $\varphi(1) = 1$. Si $n = p^\alpha$, con p primo, entre los p^α números $1, 2, \dots, p^\alpha$, sólo los de valor mp , donde $m = 1, \dots, p^{\alpha-1}$, no son primos con p . Luego:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

Si $n (\neq 1)$ no es potencia de un primo, podrá escribirse en la forma $n = rs$, con r y s primos entre sí ($r > 1, s > 1$). Todo entero x inferior o igual a n y primo con n es estrictamente inferior a n , $x < n$, y puede ponerse:

$$x = qr + y \quad (0 \leq y < r)$$

donde el resto y tiene uno de los valores $0, 1, \dots, r-1$, y el cociente q uno de los valores $0, 1, \dots, s-1$. Para que x sea primo con rs , es necesario y suficiente que sea a la vez primo con r y primo con s (esto resulta inmediatamente descomponiéndoles en factores primos). Ahora bien, para que x sea primo con r , es necesario y suficiente que y lo sea, y esto ocurre para $\varphi(r)$ valores de y .

Para un valor fijo y_0 de y , x es primo con s si lo es su resto z , módulo s . Ahora, los s números $x_q = qr + y_0$ ($q = 0, 1, \dots, s-1$) dan módulo s , s restos distintos; en efecto, la igualdad

$$x_q - x_j = (q - j)r = \lambda s$$

exige, ya que s es primo con r por hipótesis, que s divida a $q - j$, lo que sucede sólo en el caso en que $q = j$, de donde $x_q = x_j$. Esos s restos son, pues los números $0, 1, \dots, s-1$ tomados en un cierto orden y de ellos hay $\varphi(s)$ primos con s .

Por esto, finalmente, a cada uno de los $\varphi(r)$ valores de y tales que x sea primo con r corresponden $\varphi(s)$ valores de q tales que x sea primo con s ; tenemos en consecuencia

$$\varphi(rs) = \varphi(r) \cdot \varphi(s) \quad \text{supuesto} \quad \text{m.c.d.}(r, s) = 1.$$

Resulta inmediatamente, que si descompuesto n en factores primos es

$$n = p_1^{\alpha_1} \dots p_h^{\alpha_h}$$

el indicador de n vale

$$\varphi(n) = \varphi(p_1^{\alpha_1} \dots p_h^{\alpha_h}) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_h}\right).$$

Tomemos como grupo cíclico G de orden n el grupo G^* de las rotaciones de ángulo $k \cdot 2\pi/n$ ($k = 1, \dots, n$) en un plano, alrededor de un punto O : los generadores inversos a^λ y $a^{n-\lambda}$ de G^* producen un mismo polígono regular de n lados inscrito en el círculo-unidad, e inversamente a cada polígono regular de n lados corresponde la generación de G^* por dos generadores inversos.

El número de los polígonos regulares distintos de n lados, inscritos en un círculo dado, con un vértice A fijo, es pues $\frac{1}{2}\varphi(n)$.

§ 4. Grupos de tipo finito

Llamamos *grupo de tipo finito* un grupo que admite un sistema *finito* de generadores $A = \{a_1, a_2, \dots, a_n\}$. Un grupo de orden finito, un grupo monógeno (cíclico o no) son grupos de tipo finito.

Teorema 1. — *Todo sistema M de generadores de un grupo G de tipo finito contiene un subconjunto finito que es un sistema irreducible de generadores.*

El grupo de tipo G es engendrado por el sistema finito de generadores $A = \{a_1, a_2, \dots, a_n\}$. Si consideramos ahora el sistema de generadores M , cada a_i , es, de algún modo un producto de potencias positivas o negativas de un número finito de elementos $m_{i_1}, m_{i_2}, \dots, m_{i_\lambda}$ tomadas en M .

Pongamos:

$$M_i = \{m_{i_1}, \dots, m_{i_\lambda}\}, \quad M^* = \bigcup_{i=1}^n M_i.$$

M^* es un subconjunto finito de M . Por ser todo elemento de G un producto de potencias positivas o negativas de un número finito de elementos tomados en A , es también un producto de potencias positivas o negativas de elementos tomados en M^* : M^* es, pues, un sistema *finito* de generadores.

Si ningún elemento x de M^* es superfluo, es decir no pertenece al grupo engendrado por $M^* - \{x\}$, M^* es irreducible. En el caso contrario, M^* admitirá al menos un elemento superfluo s , y $M^* - \{s\} = M_1^*$ es un sistema de generadores de G , con un elemento menos que M^* . Reiterando el proceso, al fin de un número finito de operaciones, se obtendrá un sistema irreducible de generadores extraído de M^* , finito y contenido en M .

Teorema 2. — *Cualquier imagen homomorfa de un grupo de tipo finito es de tipo finito.*

Sea G un grupo engendrado por el conjunto finito $A = \{a_1, a_2, \dots, a_n\}$, $\bar{G} = h(G)$ una imagen homomorfa de G , $\bar{a}_i = h(a_i)$ las imágenes de a_i . Conside-

remos un elemento arbitrario $\bar{a}$ de $\bar{G}$ y uno de los elementos a de G del cual es la imagen: $h(a) = \bar{a}$. Tenemos:

$$a = a_{i_1}^{\alpha_1} \dots a_{i_p}^{\alpha_p} \quad (a_{i_\lambda} \in A; \alpha_\lambda \in \mathbf{Z})$$

y por consiguiente

$$\bar{a} = h(a) = \bar{a}_{i_1}^{\alpha_1} \dots \bar{a}_{i_p}^{\alpha_p}$$

El conjunto $\bar{A} = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n\}$ es pues un sistema finito de generadores para $\bar{G}$ y $\bar{G}$ es de tipo finito.

Caso particular. — Si G es monógeno, $n = 1$, también $\bar{G}$ lo es: *cualquier imagen homomorfa de un grupo monógeno es un grupo monógeno.*

Teorema 3. — *Cualquier grupo infinito de tipo finito G es numerable.*

Llamemos *longitud* l de un elemento x de G el valor *mínimo* de la suma $|\alpha_1| + \dots + |\alpha_p|$ en las diferentes representaciones posibles del elemento x bajo la forma:

$$x = a_{i_1}^{\alpha_1} \dots a_{i_p}^{\alpha_p} \quad (a_{i_\lambda} \in A, \alpha_\lambda \in \mathbf{Z}).$$

No hay más que un número finito de formas de escribir en la forma de suma, $l = l_1 + \dots + l_p$ ($p \geq 1, l_i > 0$) y, para cada una de ellas no hay en G más que un número finito de elementos de la forma

$$a_{i_1}^{\alpha_1} \dots a_{i_p}^{\alpha_p}$$

donde $\alpha_\lambda = \pm l_\lambda$. Tal elemento es de longitud a lo más l . Por consiguiente, el conjunto de los elementos de G con longitud $\leq l$ es finito, el conjunto G_l de los elementos de longitud l es también finito, y

$$G = \bigcup_{l=1}^{\infty} G_l,$$

infinito por hipótesis, resulta numerable.

Observación. — Según el teorema precedente, cualquier subgrupo de un grupo de tipo finito es numerable o finito. Pero *un subgrupo tal, no es necesariamente de tipo finito.*

Al contrario, cualquier subgrupo de un grupo *abeliano* de tipo finito es también de tipo finito, como veremos más adelante.

Insistamos también en que hay, desde luego, grupos infinitos numerables

que no son de tipo finito. Tal es, por ejemplo, el grupo *multiplicativo* $G = \mathbb{Q}^+$ de los racionales positivos. Todo elemento x de G se escribe en efecto, de una forma y de una sola, bajo la forma

$$(1) \quad x = \frac{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}{p_1'^{\alpha_1'} \cdots p_s'^{\alpha_s'}}$$

en donde las α_i y las α_j' son enteros positivos, las p_i y las p_j' números primos distintos.

Los números primos forman un sistema de generadores infinito, que es irreducible, por lo que, el grupo G no puede ser de tipo finito, según el teorema 1.

§ 5. Inmersión de un semigrupo abeliano con ley de simplificación en un grupo

Junto al sistema *irreducible* de generadores constituido por el conjunto de números primos, el grupo multiplicativo $G = \mathbb{Q}^+$ de los números racionales positivos admite el sistema de generadores $\mathbf{N} = \{1, 2, \dots, n, \dots\}$. Aunque sea reducible este sistema de generadores es notable; su estructura multiplicativa es en efecto, la de un *semigrupo abeliano en el que se cumple la ley de simplificación*. Desde el punto de vista multiplicativo, el paso de $\mathbf{N}$ a $\mathbb{Q}^+$, que tiene el interés de proporcionar un ejemplo simple de grupo que no es de tipo finito, se presenta como la *construcción de un grupo engendrado por un semigrupo abeliano con ley de simplificación*; es el problema de la *inmersión de tal semigrupo S en el menor grupo que le contiene*.

De igual modo, el grupo aditivo $\mathbf{Z}$ de los enteros relativos es el menor grupo que contiene el conjunto $\mathbf{N}$ de los enteros naturales, considerado ahora como semigrupo aditivo abeliano, en el que es válida la regla de simplificación (o ley cancelativa).

Mostraremos aquí, de forma general, que *dado un semigrupo abeliano S en que se cumple la regla de simplificación, existe un grupo mínimo Γ que contiene un semigrupo Σ isomorfo con S* (puede convenirse después, en "identificar" S y Σ); la expresión *mínimo grupo* debe entenderse aquí de la forma siguiente: ningún subgrupo propio de Γ tiene la propiedad de contener el semigrupo Σ isomorfo con S .

La demostración de ese teorema importante no es en realidad otra cosa que una generalización inmediata de la teoría elemental de las fracciones consideradas desde el solo punto de vista multiplicativo.

Expresemos multiplicativamente la ley de composición del semigrupo S y

consideremos el conjunto $\Delta = S \times S$ de los pares (a, b) de los elementos de S , con la ley de composición (cfr. cap. I, § 4, 2.º);

$$(a, b) (a', b') = (aa', bb').$$

Por otra parte introduzcamos en Δ la relación ξ definida por:

$$(a, b) \xi (a_1, b_1) \quad \text{si} \quad ab_1 = a_1b.$$

Esta relación es claramente reflexiva y simétrica: es también transitiva, pues si tenemos:

$$ab_1 = a_1b \quad \text{y} \quad a_1b_2 = a_2b_1$$

se deduce

$$ab_1b_2 = a_1bb_2 \quad \text{y} \quad a_1b_2b = a_2b_1b,$$

de donde, por ser S abeliano y cumplirse la ley cancelativa

$$ab_2 = a_2b.$$

ξ es, pues, una relación de equivalencia en Δ ; por otra parte ξ es compatible con la ley de composición de (Δ) , ya que:

$$(a, b) (x, y) \equiv (a_1, b_1) (x, y) \quad (\xi)$$

se escribe

$$(ax, by) \equiv (a_1x, b_1y) \quad (\xi)$$

es decir

$$ax b_1y = by a_1x$$

que se verifica, para cualquier $(x, y) \in \Delta$, siempre que

$$(a, b) \equiv (a_1, b_1) \quad (\xi)$$

Sea ahora Δ/ξ el semigrupo cociente, abeliano como Δ . Vamos a ver que Δ/ξ es el grupo buscado.

Es inmediato que los pares (m, m) ($m \in S$) forman una clase E módulo ξ ; E es elemento unidad de Δ/ξ ya que en Δ , para cualquier par (a, b) , tendremos:

$$(a, b) (m, m) = (am, bm) \equiv (a, b) \quad (\xi)$$

de donde en $\Delta/\mathcal{E}$ designando por X la clase del par (a, b) resulta

$$XE = X \quad \forall X \in \Delta/\mathcal{E}$$

Por otra parte X tiene como inversa la clase X^{-1} que contiene al par (b, a) ya que tenemos, en Δ ,

$$(a, b)(b, a) = (ab, ab) \in E$$

de donde, en $\Delta/(\mathcal{E})$

$$XX^{-1} = E.$$

En consecuencia, $\Delta/\mathcal{E}$ es un *grupo* abeliano Γ .

Dado un elemento a de S , el conjunto A de los pares (am, m) donde m recorre a S , es una clase módulo $\mathcal{E}$. Tenemos en efecto por lo pronto

$$(am, m) \equiv (am', m') \quad (\mathcal{E})$$

Recíprocamente, puesto que la igualdad $amy = mx$ implica $x = ay$, un par (x, y) equivalente a (am, m) se escribe (ay, y) . La aplicación

$$(\varphi) \quad a \rightarrow A$$

es una aplicación biyectiva de S sobre el conjunto Σ de las clases A ; φ es, incluso, un *isomorfismo* puesto que tenemos, en Δ ,

$$(am, m)(a'm', m') = (aa' \cdot mm', mm').$$

El grupo Γ contiene pues, efectivamente un subsemigrupo Σ isomorfo al semigrupo dado S .

Supongamos ahora que una parte estable Γ' de Γ , que contiene Σ , sea el mismo un *grupo* (con la ley de composición de Γ restringida a Γ') y demostremos que necesariamente tendremos $\Gamma' = \Gamma$. Sea X un elemento de Γ ; X es una clase de pares (a, b) , ..., y si designamos por A la clase que contiene al par (am, m) , y por B la clase que contiene el par (bm, m) , X contiene al par

$$(a, b) \equiv (am, m)(m, bm) \quad (\mathcal{E})$$

y en consecuencia tenemos en Γ la igualdad

$$X = AB^{-1}$$

Pero, $A \in \Sigma$, $B \in \Sigma$ y $\Sigma \subseteq \Gamma'$ deduciéndose que $A \in \Gamma'$, $B^{-1} \in \Gamma'$, luego $AB^{-1} = X \in \Gamma'$, de donde necesariamente $\Gamma' = \Gamma$; vemos así que Γ no admite como subgrupo propio que contiene el semigrupo Σ isomorfo con S .

§ 6. Grupos libres

Sea $\mathcal{M}$ un conjunto no vacío de elementos que por comodidad llamamos *letras*, $\mathcal{M} = \{a, b, \dots\}$. Asociemos a $\mathcal{M}$ un conjunto $\mathcal{M}'$ correspondiéndole biyectivamente (biunívocamente); sea x' la imagen, en $\mathcal{M}'$, del elemento x de $\mathcal{M}$: diremos que x y x' son asociados.

Toda expresión

$$W = cb'da'c'a$$

obtenida escribiendo las letras de $\mathcal{M}$ o de $\mathcal{M}'$, en número finito, unas a continuación de otras, se llama una *palabra*. Una palabra depende pues de las letras que figuran (cada letra puede figurar varias veces) y del orden en el cual están escritas. Consideremos igualmente la *palabra vacía*, $\emptyset$, que no contiene ninguna letra.

Una palabra es *reducida* cuando no contiene pares de letras asociadas consecutivas: $ac'b$ es reducida, $acc'd'db$, $acd'dc'b$ no lo son. En una palabra no reducida W , se puede suprimir los pares de elementos asociados consecutivos, y después repetir esta operación sobre las palabras sucesivamente obtenidas, tantas veces como sea posible. Se llega así al menos de una manera a una palabra reducida (eventualmente vacía).

Dos palabras reducidas son *iguales* si están constituidas por las mismas letras en el mismo orden.

Consideremos el conjunto $\mathcal{E}$ de las palabras reducidas (comprendida la vacía) que se pueden escribir con los elementos letras de $\mathcal{M}$ y las letras asociadas elementos de $\mathcal{M}'$. Definimos en $\mathcal{E}$ una ley de composición interna $\mathbf{T}$ de la manera siguiente:

Sean

$$A = a_1^* a_2^* \dots a_p^*, \quad B = b_1^* b_2^* \dots b_q^*$$

dos palabras reducidas; $a_i^*, b_j^* \in \mathcal{M} \cup \mathcal{M}'$ y la estrella $*$ en a_i^* representa una de estas dos cosas: el acento $'$ si $a_i^* \in \mathcal{M}'$, nada si $a_i^* \in \mathcal{M}$. Escribiendo la palabra B después de la A obtendremos la palabra

$$AB = a_1^* a_2^* \dots a_p^* b_1^* b_2^* \dots b_q^*$$

que es reducida si a_p^* y b_1^* no son asociados, y solamente en ese caso. Si a_p^* y b_1^* son asociados, los suprimimos y la palabra así obtenida es reducida si a_{p-1}^* y b_2^* no son asociados, y solamente en ese caso. Siguiendo con esta reducción hasta el fin, obtenemos después de un número finito de operaciones una palabra reducida $R(AB)$ que designamos por $A \top B$. En resumen la ley de composición $\top$ se define por

$$A \top B = R(AB).$$

Tenemos evidentemente

$$A \top \emptyset = \emptyset \top A = A \quad \forall A \in \mathcal{E}.$$

Sea A^{-1} la palabra formada con las asociadas de las letras de A escritas en el orden opuesto; A^{-1} es reducida si A lo es, y recíprocamente; tenemos

$$R(AA^{-1}) = \emptyset, \quad \text{es decir} \quad A \top A^{-1} = \emptyset$$

y lo mismo $A^{-1} \top A = \emptyset$. Asignándole la ley $\top$ el conjunto $\mathcal{E}$ de las palabras reducidas posee pues un elemento neutro $\emptyset$ y existe para todo elemento A de $\mathcal{E}$ un inverso A^{-1} .

Demostremos que $\mathcal{E}$, con ley de composición $\top$, es un grupo, que es, por definición, el *grupo libre* engendrado por $\mathcal{M}$: es suficiente establecer la propiedad asociativa de $\top$.

$$(A \top C) \top B = A \top (C \top B) \quad \forall A, B, C \in \mathcal{E}.$$

Esta igualdad es evidente si C es la palabra vacía. Consideremos ahora el caso en que C es una palabra de una sola letra, $C = c^*$; acabaremos la demostración razonando por recurrencia sobre la *longitud* de la palabra reducida C , es decir sobre el número de sus letras.

Escribiendo $A = A_1 a^*$, $B = b^* B_1$, tendremos

$$(A \top c^*) \top B = R\{[R(A_1 a^* c^*)] b^* B_1\},$$

$$A \top (c^* \top B) = R[A_1 a^* R(c^* b^* B_1)].$$

Hay que distinguir ahora los cuatro casos posibles:

1. c^* no es asociado ni de a^* ni de b^* : los segundos miembros son entonces, $A_1 a^* c^* b^* B_1 = A c^* B$;
2. c^* es asociado de a^* y de b^* , lo que exige $a^* = b^*$; los dos segundos miembros son $A_1 a^* B_1$;

3. c^* es asociado de a^* , pero no de b^* ; los dos segundos miembros son, en este caso $R(A_1 b^* B_1) = R(A_1 B)$;

4. c^* es asociado de b^* , pero no de a^* ; los dos segundos miembros son $R(A_1 a^* B_1) = R(A B_1)$.

En todos los casos hemos obtenido efectivamente la igualdad

$$(A \top c^*) \top B = A \top (c^* \top B)$$

que expresa la asociatividad en el caso en que C es una palabra de una sola letra.

Supongamos ahora que C sea una palabra reducida de n letras, y que la asociatividad sea válida cuando la palabra intermedia tenga $n - 1$ letras. Escribamos $C = C'c^*$, donde C' es una palabra reducida de $n - 1$ letras.

Así tendremos

$$C = C' \top c^*,$$

lo que permite escribir:

$$\begin{aligned} (A \top C) \top B &= [A \top (C' \top c^*)] \top B \\ &= [(A \top C') \top c^*] \top B \\ &= (A \top C') \top (c^* \top B) \\ &= A \top [C' \top (c^* \top B)] \\ &= A \top [(C' \top c^*) \top B] = A \top (C \top B) \end{aligned}$$

y la proposición queda establecida.

Las palabras de una sola letra son, desde luego, palabras reducidas. Una palabra cualquiera W puede considerarse como una sucesión de n palabras reducidas:

$$W = R_1 R_2 \dots R_n$$

formadas por sus n letras sucesivas. Cualquier procedimiento que permita pasar de W a una palabra reducida por supresión de letras consecutivas asociadas equivale al cálculo de la palabra:

$$R_1 \top R_2 \top \dots \top R_n,$$

realizándose este cálculo conforme a un cierto sistema de paréntesis, corche.

tes, etc. Como la operación $\mathbf{T}$ es asociativa, el resultado final es independiente del modo de operar y se obtiene siempre *la misma palabra reducida*, que llamaremos *reducida* de W y designaremos por $R(W)$.

En el conjunto $\mathcal{W}$ de todas las palabras formadas por un alfabeto dado $\mathcal{M}$, consideremos la relación ρ definida por:

$$W \rho W' \quad \text{si} \quad R(W) = R(W');$$

ρ es visiblemente una relación de equivalencia. Además, esta relación de equivalencia es *compatible* con la ley de composición que, partiendo de dos palabras W_1, W_2 de $\mathcal{W}$, da como resultado la palabra $W_1 W_2$, que se obtiene al escribir W_2 a continuación de W_1 . Para formar efectivamente la palabra reducida $R(W_1 W_2)$, se pueden reducir W_1 y W_2 , separadamente, después formar la palabra $R(W_1)R(W_2)$, y, en fin, reducir esta última: por lo tanto $R(W_1 W_2)$ depende sólo de $R(W_1)$ y $R(W_2)$, y en consecuencia

$$W_i \equiv W'_i \quad (\rho) \quad (i = 1, 2)$$

implica

$$W_1 W_2 \equiv W'_1 W'_2 \quad (\rho).$$

Puesto que en el conjunto $\mathcal{E}$ de palabras reducidas, la ley $\mathbf{T}$ se define por

$$A \mathbf{T} B = R(AB),$$

la aplicación

$$W \rightarrow R(W)$$

de $\mathcal{W}$ sobre $\mathcal{E}$ es un *homomorfismo* para la ley considerada en $\mathcal{W}$ y para la ley $\mathbf{T}$ de $\mathcal{E}$; el núcleo de este homomorfismo es el conjunto de palabras que tienen por reducida la palabra vacía.

Ejemplos. — I. Cuando $\mathcal{M}$ se compone de una sola letra $\mathcal{M} = \{a\}$, el grupo libre $\mathcal{E}$ está formado por la palabra vacía y las palabras reducidas $aa \dots a$, $a'a' \dots a'$. $\mathcal{E}$ es isomorfo con el grupo aditivo $\mathbf{Z}$ de los enteros; la palabra formada por p letras a tiene por imagen $+p$, la palabra formada de q letras a' tiene por imagen $-q$. Es pues un grupo monógeno *infinito*.

II. Sea ahora un $\mathcal{M}$ cualquiera. Si $A = a_1^* \dots a_p^*$ es una palabra reducida, tendremos $A = a_1^* \mathbf{T} a_2^* \mathbf{T} \dots \mathbf{T} a_p^*$. Convengamos en escribir a^n para la palabra formada de n letras a , y a^{-m} para la palabra formada de m letras a' . Podremos

entonces, en el grupo $\mathfrak{E}$, pasar a la notación multiplicativa: Cada elemento del grupo libre $\mathfrak{E}$ se escribe de una manera única como producto finito de potencias positivas o negativas de elementos de $\mathcal{M}$, es decir, como *producto de elementos de los grupos monógenos engendrados por los elementos de $\mathcal{M}$* . Se dice que los elementos de $\mathcal{M}$ son los *generadores* del grupo libre $\mathfrak{E}$, y que $\mathfrak{E}$ es el *producto libre de los grupos monógenos engendrados por los elementos de $\mathcal{M}$* . Se llama *rango* del grupo libre $\mathfrak{E}$, el número (finito o infinito) de sus generadores, es decir, el número de elementos de $\mathcal{M}$.

Teorema fundamental. — *Todo grupo G es isomorfo a un grupo cociente de un grupo libre.*

Sea $\mathcal{S}$ un sistema de generadores del grupo G . Consideramos el grupo libre Γ engendrado por un sistema de generadores $\mathcal{M}$ tal, que exista una aplicación biyectiva φ de $\mathcal{M}$ sobre $\mathcal{S}$. A todo elemento

$$a = a_{i_1}^{\alpha_1} a_{i_2}^{\alpha_2} \dots a_{i_r}^{\alpha_r} \in \Gamma \quad (a_{i_\lambda} \in \mathcal{M}, \alpha_\lambda \in \mathbb{Z} - \{0\})$$

asociemos en G el elemento

$$x = \Phi(a) = s_{i_1}^{\alpha_1} s_{i_2}^{\alpha_2} \dots s_{i_r}^{\alpha_r} \quad \text{donde} \quad s_{i_\lambda} = \varphi(a_{i_\lambda}) \in \mathcal{S}$$

Esta aplicación Φ de Γ sobre G tiene las siguientes propiedades: *Prolonga* a φ (es decir, su restricción a $\mathcal{M}$ es la aplicación φ de $\mathcal{M}$ sobre $\mathcal{S}$); es *exhaustiva* (todo elemento de G resulta obtenido como imagen), puesto que $\mathcal{S}$ es un sistema de generadores de G y la propia φ es una aplicación exhaustiva. Finalmente, por construcción,

$$\Phi(ab) = \Phi(a) \cdot \Phi(b)$$

Según las dos últimas propiedades, Φ es un *homomorfismo* que aplica el grupo libre Γ sobre el grupo G dado. Utilizando el teorema del homomorfismo, podremos escribir

$$(1) \quad G \simeq \Gamma/N$$

donde N designa el núcleo del homomorfismo Φ , subgrupo distinguido de Γ .

La representación precedente (1) depende, desde luego, del sistema de generadores $\mathcal{S}$ elegido en G . En particular, se ve que *un grupo G con un sistema de generadores de m elementos (grupo de tipo finito) es isomorfo a un grupo cociente de un grupo libre de rango m .*

Cualquier elemento n de N , como palabra de Γ es de la forma

$$n = a_{i_1}^{\alpha_1} a_{i_2}^{\alpha_2} \dots a_{i_r}^{\alpha_r} \quad (a_{i_\lambda} \in \mathcal{M}, \alpha_\lambda \in \mathbb{Z} - \{0\}).$$

Tomando su imagen $\Phi(n) = e$, obtenemos

$$(2) \quad s_{i_1}^{\alpha_1} s_{i_2}^{\alpha_2} \dots s_{i_r}^{\alpha_r} = e \quad (s_i \in \mathcal{S})$$

que es una relación entre ciertos generadores $s_{i_1}, \dots, s_{i_r}$ de G .

Si N_0 es un sistema de generadores para N , el conjunto de relaciones (2) obtenidas para todos los elementos n de N es una consecuencia del subconjunto (D) formado por aquellas relaciones (2) que provienen de los elementos de N_0 . Las relaciones (D) se llaman *relaciones de definición* (o *relaciones fundamentales*) del grupo G , para el sistema de generadores $\mathcal{S}$.

Además, si se toma para sistema de generadores N_0 de N un sistema *irreducible*, ningún elemento de N_0 se expresará en forma de producto de potencias positivas o negativas de un número finito de otros elementos de N_0 . En consecuencia, ninguna de las relaciones de definición del sistema correspondiente (D) es combinación de un número finito de otras por multiplicación miembro a miembro y paso a las inversas. En este caso diremos que (D) es un *sistema irreducible de relaciones de definición*.

Si para definir al grupo G se conocen un conjunto de generadores $\mathcal{S}$ y un sistema de relaciones (D) entre los generadores, $\mathcal{M}$ queda definido a menos de una biyección, y el grupo libre Γ queda definido salvo isomorfismos; el conjunto N_0 de los elementos $a_{i_1}^{\alpha_1} a_{i_2}^{\alpha_2} \dots a_{i_r}^{\alpha_r}$ de Γ que corresponden a los primeros miembros $s_{i_1}^{\alpha_1} s_{i_2}^{\alpha_2} \dots s_{i_r}^{\alpha_r}$ de las relaciones (D) está perfectamente definido, así como el subgrupo distinguido N de (D) que N_0 engendra (N es la clausura de N_0 en la familia de Moore de los subgrupos distinguidos de Γ). Finalmente, Γ/N está definido salvo isomorfismos y, según (1), también G . Existe pues un grupo G determinado salvo isomorfismos, que admite el conjunto de generadores $\mathcal{S}$ y el sistema de relaciones D como relaciones de definición.

Supongamos ahora que para dos grupos G, G' que admiten el mismo conjunto de generadores $\mathcal{S}$, se tengan respectivamente dos sistemas de relaciones de definición (D), (D'), deduciéndose (D') de (D) por la adjunción de ciertas relaciones suplementarias. Tendremos

$$G \simeq \Gamma/N, \quad G' \simeq \Gamma/N'$$

donde N, N' son los subgrupos distinguidos del grupo libre Γ definidos como antes se ha visto a partir de (D) y (D'). Resulta $N \subseteq N' (\subseteq \Gamma)$ y N es *a fortiori* subgrupo distinguido de N' . Según el primer teorema de isomorfismo se tiene

$$\Gamma/N' \simeq \Gamma/N/N'.$$

Ahora bien, en el isomorfismo $\Gamma/N \simeq G$, la imagen de N'/N es un cierto subgrupo distinguido H de G , y por lo tanto

$$\Gamma/N/N'/N \simeq G/H$$

de donde finalmente

$$G' \simeq \Gamma/N' \simeq G/H$$

y podemos enunciar:

Teorema (de von Dyck). — Si dos grupos G y G' admiten un mismo conjunto de generadores S y están dados por sendos sistemas de relaciones de definición (D) , (D') , donde (D') se compone de (D) y de ciertas relaciones suplementarias, G' es isomorfo a un grupo cociente de G .

Si $N' = N$, resulta $G' \simeq G$. La igualdad $N' = N$ expresa de modo preciso el hecho de que las relaciones adjuntadas a (D) para formar (D') son “superfluas”.

§ 7. Grupos abelianos libres

Se llama *grupo abeliano libre* un grupo Γ en el que las únicas relaciones de definición expresan la conmutatividad:

$$aba^{-1}b^{-1} = e \quad \forall a, b \in \Gamma$$

(en notación multiplicativa).

Consecuencias. — 1) Todo elemento de Γ engendra un subgrupo monógeno infinito.

2) Todos los generadores engendran grupos monógenos en los que la unidad, e , es el único elemento común.

3) Cualquier elemento del grupo abeliano libre Γ es una *palabra* formada con la ayuda de los generadores $a, b, \dots$ y de sus asociados, $a^{-}, b^{-} \dots$ que se pueden escribir en un orden elegido *a priori*, por ejemplo $a^{*\alpha} b^{*\beta} \dots l^{*\lambda}$, siendo $\alpha, \beta, \dots, \lambda$ enteros no negativos, y a^{*} representa a uno de los dos elementos a, a^{-} y figura en la palabra una vez a lo más.

En notación aditiva, todo elemento α de Γ se escribe de una manera, y sólo de una, como $\sum_i k_i a_i$, siendo Σ una suma finita, las a_i generadores de Γ y las k_i enteros positivos o negativos.

Teorema 1. — *Todo grupo abeliano G es isomorfo a un grupo cociente de un grupo abeliano libre.*

Sea efectivamente $\mathcal{S}$ un sistema de generadores de G . Consideremos el grupo abeliano libre Γ (aditivo) engendrado por un sistema de generadores $\mathcal{M}$ que corresponde a $\mathcal{S}$ por una biyección φ . Sea una palabra $\sum_i k_i a_i \in \Gamma$. Asociemos a ésta en G el elemento

$$\sum_i k_i s_i, \quad \text{donde } s_i = \varphi(a_i) \in \mathcal{S};$$

como φ es una biyección de $\mathcal{M}$ sobre $\mathcal{S}$, la aplicación de Γ en G definida así es *exhaustiva*. Además, por construcción, si u y v son dos elementos de Γ , se tiene

$$\varphi(u + v) = \varphi(u) + \varphi(v),$$

luego φ es un *homomorfismo* que aplica el grupo abeliano libre Γ sobre el grupo dado G . Según el teorema del homomorfismo tendremos

$$G \simeq \Gamma / N$$

donde N , núcleo del homomorfismo φ es un subgrupo de Γ .

CAPÍTULO IV

ANILLOS Y CUERPOS

§ 1. Leyes de composición distributivas

A un conjunto E con diversas leyes de composición $\top$, $\perp$, ... se le llama con frecuencia *álgebra* (o *dominio*). Entre las leyes de composición que operan en un mismo conjunto, se encuentra frecuentemente una propiedad importante, esto es, el carácter *distributivo* de una ley con relación a otra.

Definiciones. — La ley $\perp$ es *distributiva a la izquierda con respecto a la ley $\top$* si:

$$(1) \quad a \perp (x \top y) = (a \perp x) \top (a \perp y) \text{ cualesquiera sean } a, x, y \in E$$

y, análogamente, es *distributiva a la derecha* si:

$$(1') \quad (x \top y) \perp a = (x \perp a) \top (y \perp a) \text{ cualesquiera sean } a, x, y \in E;$$

En fin, se dice que la ley $\perp$ es *distributiva con respecto a la ley $\top$* cuando ambas condiciones precedentes se cumplen. También se dice en estos casos, que la ley $\top$ es *distribuida* por la ley $\perp$. Si la ley $\perp$ es conmutativa, las tres condiciones precedentes son equivalentes.

Ejemplos. — La multiplicación de números naturales (o racionales, o reales, o complejos) es distributiva respecto a la adición, pero la adición no es distributiva respecto a la multiplicación. Se sabe también, que, en el conjunto $\mathbf{N}$ de los números naturales, la multiplicación es distributiva respecto a la formación del m.c.d. y del m.c.m., y se demuestra (utilizando por ejemplo la descomposición en factores primos) que cada una de estas dos leyes últimas es distributiva respecto a la otra. En la teoría de conjuntos se demuestra que, en el conjunto $\mathcal{P}(M)$ de

las partes de un conjunto M , la intersección $\cap$ y la unión $\cup$ son distributivas cada una respecto de la otra ¹. Si consideramos ahora el conjunto de las partes, $\mathcal{P}(E)$, de un conjunto E con la ley $\top$, (Cap. I, § 4, 4.º) las fórmulas

$$R_2 \quad A \top \left(\bigcup_{X \in \mathcal{F}} X \right) = \bigcup_{X \in \mathcal{F}} (A \top X), \quad \left(\bigcup_{X \in \mathcal{F}} X \right) \top B = \bigcup_{X \in \mathcal{F}} (X \top B),$$

expresan que la ley de composición $\top$ en $\mathcal{P}(E)$ es distributiva respecto a la unión, mientras que en general no lo es para la intersección, ya que para ésta sólo sabemos que

$$R_3 \quad A \top \left(\bigcap_{X \in \mathcal{F}} X \right) \subseteq \bigcap_{X \in \mathcal{F}} (A \top X), \quad \left(\bigcap_{X \in \mathcal{F}} X \right) \top B \subseteq \bigcap_{X \in \mathcal{F}} (X \top B),$$

expresiones en las que la inclusión, puede ser estricta.

Examinemos ahora, si los principales métodos para definir nuevas leyes de composición a partir de leyes dadas, conservan la propiedad distributiva.

1.º Sea E un conjunto con una primera ley de composición $\top$ cualquiera, y una segunda ley $\cdot$ distributiva respecto a $\top$. El conjunto $\mathcal{F}$ de las funciones f

¹ Sean, de modo general, A una parte cualquiera de M y $\mathcal{F}$ una familia finita o infinita de partes de M . Se tiene

$$A \cap \left(\bigcup_{X \in \mathcal{F}} X \right) = \bigcup_{X \in \mathcal{F}} (A \cap X),$$

$$A \cup \left(\bigcap_{X \in \mathcal{F}} X \right) = \bigcap_{X \in \mathcal{F}} (A \cup X).$$

Sea, en efecto,

$$x_0 \in A \cap \left(\bigcup_{X \in \mathcal{F}} X \right);$$

Tendremos $x_0 \in A$ y existe al menos una parte $X_0 \in \mathcal{F}$ tal que $x_0 \in X_0$; entonces $x_0 \in A \cap X_0$, de donde

$$x_0 \in \bigcup_{X \in \mathcal{F}} A \cap X;$$

y recíprocamente, si

$$x_1 \in \bigcup_{X \in \mathcal{F}} (A \cap X),$$

existirá al menos una parte $X_1 \in \mathcal{F}$ tal que $x_1 \in A \cap X_1$, de donde $x_1 \in A$ y $x_1 \in X_1$, luego

$$x_1 \in \bigcup_{X \in \mathcal{F}} X$$

y en fin,

$$x_1 \in A \cap \left(\bigcup_{X \in \mathcal{F}} X \right).$$

con esto se establece la primera igualdad, ya que cada uno de los dos miembros está contenido en el otro.

definidas sobre un conjunto dado X y tomando valores en E , tiene dos leyes correspondientes designadas igualmente por $\top$ y $\cdot$ (cap. I, § 4, 1.º).

Es claro que, en $\mathcal{F}$, la ley de composición $\cdot$ es distributiva respecto a $\top$:

$$(f \top g) \cdot h = (f \cdot h) \top (g \cdot h) \quad \forall f, g, h \in \mathcal{F}$$

(para la ley distributiva a la derecha por ejemplo), puesto que en E tendremos, para todo elemento x de X :

$$[f(x) \top g(x)] \cdot h(x) = [f(x) \cdot h(x)] \top [g(x) \cdot h(x)].$$

2.º Sean igualmente E_1 , E_2 dos conjuntos con dos leyes de composición cada uno, que para más comodidad denotaremos aditiva y multiplicativamente, siendo cada multiplicación distributiva respecto a la adición del mismo conjunto.

Como se ha visto (cap. I, § 4, 2.º) se deducen una multiplicación y una adición en el conjunto producto $E_1 \times E_2 = P$, y esta multiplicación es distributiva respecto a la adición, según muestra la serie de igualdades:

$$\begin{aligned} (a_1, a_2) [(b_1, b_2) + (b'_1, b'_2)] &= [a_1(b_1 + b'_1), a_2(b_2 + b'_2)] \\ &= (a_1b_1 + a_1b'_1, a_2b_2 + a_2b'_2) = (a_1, a_2) (b_1, b_2) + (a_1, a_2) (b'_1, b'_2). \end{aligned}$$

3.º Resulta evidente que si E es un conjunto con una adición y una multiplicación distributiva respecto de aquella, y A es una parte de E estable para esas dos operaciones, la restricción a A de la multiplicación de E será distributiva respecto a la restricción a A de la adición de E .

4.º Siendo E , como siempre, un conjunto con una adición y una multiplicación distributiva respecto de esa adición, la extensión de estas dos operaciones al conjunto de las partes $\mathcal{P}(E)$ no conserva en general la propiedad distributiva. Para verlo consideremos que E sea el conjunto $\mathbf{Z}$ de los números enteros (≥ 0) con la adición y la multiplicación ordinarias, y sean las partes

$$A = \{0, 1\}, \quad B = \{b\}, \quad C = \{c\}, \quad \text{donde } b \neq 0, \quad c \neq 0.$$

Tendremos

$$A(B + C) = \{0, b + c\}, \quad AB + AC = \{0, b, c, b + c\}$$

y, por lo tanto, $A(B + C) \subset AB + AC$ estrictamente.

En cuanto a la segunda igualdad, es obvio que todo elemento de A pertenece a los dos miembros; y para un elemento x no situado en A , pertenecer a uno cualquiera de los dos miembros equivale a: $x \in X, \forall X \in \mathcal{F}$.

De un modo general, para tres partes cualesquiera A, B, C , de E , tendremos:

$$\begin{aligned} A(B + C) &= \{ a(b + c); a \in A, b \in B, c \in C \} \\ &= \{ ab + ac; a \in A, b \in B, c \in C \} \end{aligned}$$

$$AB + AC = \{ ab + a'c; a \text{ y } a' \in A, b \in B, c \in C \},$$

luego, en todo caso

$$A(B + C) \subseteq AB + AC.$$

5.º Teniendo E la misma significación, sea $\mathcal{F}$ una familia de Moore de partes de E con las leyes de composición $\bar{+}$ y $\bar{\cdot}$ definidas mediante la clausura, a partir de la adición y la multiplicación de E como se ha visto en el capítulo primero (§ 4, 5.º). En general la ley $\bar{\cdot}$ no es distributiva respecto a la ley $\bar{+}$: en efecto si tomamos $\mathcal{F} = \mathcal{I}(E)$, nos encontramos en el caso precedente, siendo $\bar{+}$ la adición de las partes y $\bar{\cdot}$ su multiplicación. Por lo demás, de forma totalmente general se tiene:

$$F \bar{\cdot} (F_1 \bar{+} F_2) = \overline{F \cdot (F_1 + F_2)}$$

y

$$(F \bar{\cdot} F_1) \bar{+} (F \bar{\cdot} F_2) = \overline{F \cdot F_1 + F \cdot F_2}.$$

6.º En un conjunto E con una adición y una multiplicación que supondremos, por ejemplo, *distributiva a la izquierda* respecto a la adición, consideremos una relación de equivalencia $\mathcal{R}$ compatible con esas dos leyes de composición. Como se ha visto en el capítulo primero (§ 4, 6.º), se define entonces, en el conjunto cociente $E/\mathcal{R}$, una adición y una multiplicación de las clases $X, Y, \dots$. En $E/\mathcal{R}$, la multiplicación es distributiva a la izquierda respecto a la adición. Sean en efecto A, B, C , tres clases cualesquiera (distintas o no) y a, b, c , tres elementos de E , que pertenecen respectivamente a estas clases. La clase $A(B + C)$, por definición, contiene el elemento $a(b + c)$; la clase $AB + AC$, por definición, contiene el elemento $ab + ac$. Como estos dos elementos son iguales, las dos clases coinciden:

$$A(B + C) = AB + AC.$$

Se tiene un resultado análogo para la propiedad distributiva a la derecha, y por consiguiente, para la propiedad distributiva: *El carácter distributivo de una ley respecto a otra se conserva, pues, en el paso al cociente por una equivalencia compatible con estas leyes, y también en el paso a una imagen homomorfa.*

Si, en particular, tomamos como E el conjunto $\mathbb{Z}$ de los enteros relativos con

la adición y multiplicación ordinarias, y para $\mathcal{R}$ la congruencia aritmética $\mathcal{C}_m$ módulo m , compatible con estas dos operaciones, se ve que, *en el conjunto $\mathbf{Z}/(m)$ de las clases residuales módulo m , la multiplicación es distributiva respecto a la adición.*

Sea E otra vez, un conjunto con una adición y una multiplicación distributiva (al menos a un lado) respecto de la adición: exigiendo para la adición ciertas condiciones suplementarias, vamos a obtener algunas proposiciones sencillas, pero importantes.

Teorema 1. — *En un conjunto E con una multiplicación distributiva respecto a una adición que es asociativa, se tienen las fórmulas:*

$$(1) \quad x \left(\sum_{i=1}^m a_i \right) = \sum_{i=1}^m x a_i,$$

$$(2) \quad \left(\sum_{j=1}^n b_j \right) y = \sum_{j=1}^n b_j y,$$

$$(3) \quad \left(\sum_{\lambda=1}^r u_{\lambda} \right) \left(\sum_{\mu=1}^s v_{\mu} \right) = \sum_{\lambda, \mu=1}^{r, s} u_{\lambda} v_{\mu}.$$

Las fórmulas (1) y (2) se demuestran inmediatamente por recurrencia sobre los enteros m y n ; de ellas resulta la fórmula (3).

Nota. — A menos que la multiplicación de E sea conmutativa, el orden de los factores debe ser cuidadosamente respetado en las fórmulas (1), (2) y (3).

Teorema 2. — *Sea E un conjunto con una adición y una multiplicación distributiva a la izquierda respecto a esa adición; si hay un elemento neutro para la adición, sea 0 , y si la adición verifica la regla de la simplificación a la izquierda, 0 es lícito a la izquierda para la multiplicación:*

$$x0 = 0 \quad \forall x \in E.$$

Se tiene en efecto

$$x0 + 0 = x0 = x(0 + 0) = x0 + x0$$

de donde

$$x0 = 0.$$

Es válido el teorema simétrico, y finalmente, con la ley distributiva de la multiplicación respecto a la suma y la regla de simplificación para la adición, se deduce que un "cero aditivo" (es decir, un elemento neutro para la adición) es también un "cero multiplicativo" (es decir, un elemento lícito para la multiplicación).

Teorema 3. — *Sea E un conjunto con una adición y una multiplicación distributiva a la izquierda respecto a aquella. Si E es un grupo respecto a la adición, la multiplicación es también distributiva a la izquierda respecto a la sustracción.*

Sean a , b y x tres elementos cualesquiera de E . Pongamos

$$a - b = c;$$

tendremos

$$xa = x(c + b) = xc + xb$$

luego, en fin:

$$x(a - b) = xc = xa - xb.$$

Vale un teorema análogo para la propiedad distributiva a la derecha, y también, por lo tanto, para la distributiva bilátera.

Notaremos en fin, que cuando E sea un grupo aditivo, se cumplen las hipótesis sobre la adición de los teoremas 1 y 2. Aparece así, un tipo de estructura algebraica interesante, esto es, la de un grupo aditivo E con una multiplicación distributiva respecto a la adición del grupo. El caso más importante es aquel en el que, además, la adición es conmutativa y la multiplicación asociativa.

§ 2. Anillos. Subanillos. Grupos de las unidades

Un anillo A es un conjunto con dos leyes de composición que llamamos *adición* y *multiplicación*, cumpliendo las condiciones siguientes:

1.º A es un grupo abeliano para la adición; el elemento neutro en esta adición se llama *cero* del anillo A , y se escribe generalmente 0;

2.º A es un semigrupo para la multiplicación;

3.º La multiplicación es distributiva (a los dos lados) respecto a la adición.

Si la multiplicación es conmutativa, el anillo se llama *conmutativo*.

Si en el anillo A hay un elemento, e , neutro para la multiplicación se le llama, a este e , elemento unidad del anillo:

$$ex = xe = x \quad \forall x \in A$$

Se dice entonces, que A es un *anillo con elemento unidad*. Al elemento unidad e se le indica muy frecuentemente por 1, aunque no se trate del número 1.¹

Notas. — 1. Un anillo A *nunca es vacío*, puesto que es un grupo aditivo. A contiene siempre un elemento cero.

2. En un anillo compuesto del único elemento 0, éste es elemento unidad para la multiplicación: se ha convenido en excluir este caso cuando se habla de un anillo con elemento unidad $e : e \neq 0$.

Una aplicación *biyectiva* de un anillo A sobre un anillo A' , compatible con las adiciones y con las multiplicaciones, se llama un *isomorfismo* (de anillos).

Ejemplos. — 1. El conjunto $\mathbf{Z}$ de los *enteros relativos*, el conjunto $\mathbf{Q}$ de los *números racionales* (≥ 0), el conjunto $\mathbf{R}$ de los *números reales*, el conjunto $\mathbf{C}$ de los *números complejos*, el conjunto $\mathbf{G}$ de los *números de Gauss*, es decir de los números complejos $a + bi$ con $a, b \in \mathbf{Z}$, son anillos conmutativos con elemento unidad, 1.

2. Sean X un conjunto cualquiera, y A un anillo. El conjunto $\mathcal{F}$ de las funciones f definidas sobre X y tomando su valor en A , con la adición y la multiplicación definidas a partir de las de A por el procedimiento habitual, es un anillo. Si A es conmutativo, $\mathcal{F}$ también lo es. Si A tiene un elemento unidad e , también el anillo $\mathcal{F}$ tendrá un elemento unidad ϵ que es la función definida por:

$$\epsilon(x) = e \quad \forall x \in X,$$

mientras que el elemento cero θ de $\mathcal{F}$ es la función definida por

$$\theta(x) = 0 (\in A) \quad \forall x \in X.$$

Si X es el conjunto $\mathbf{N}$ de los números naturales, las funciones f toman el nombre de *sucesiones*, formadas con elementos de A y representadas por las notaciones

$$\{a_1, a_2, \dots, a_n, \dots\} \quad \text{o} \quad \{a_n\}, \quad \text{con} \quad a_n = f(n).$$

¹ Como es usual en español diremos siempre *elemento unidad* (que, si existe, es único) y no simplemente *unidad*, por cuanto interesa distinguir aquel concepto del de las *unidades* de un anillo, que más adelante se establece (pág. 121). La improbable confusión pudiera evitarse con un guión ("élément-unité", en el original), o llamando a e elemento *uno*, por ejemplo. (N. del T.)

Según la definición de las leyes de composición en $\mathcal{F}$, si $\alpha = \{a_n\}$ y $\beta = \{b_n\}$ son dos sucesiones, su suma y su producto son las sucesiones:

$$\alpha + \beta = \{a_n + b_n\}, \quad \alpha\beta = \{a_nb_n\},$$

resultantes de la adición y la multiplicación "término a término".

3. Si A y B son dos anillos cualesquiera el conjunto de pares (a, b) donde $a \in A$, $b \in B$ con la adición y la multiplicación definidas por

$$(a, b) + (a', b') = (a + a', b + b')$$

$$(a, b)(a', b') = (aa', bb')$$

es igualmente un anillo, llamado *anillo producto*.

4. En un anillo A , sea $\mathcal{R}$ una relación de equivalencia compatible con la suma y la multiplicación de A . Como hemos visto (cap. I, § 5) el conjunto cociente $A/\mathcal{R}$ admite una suma y una multiplicación (operando sobre las clases módulo $\mathcal{R}$); $A/\mathcal{R}$ es grupo aditivo, es semigrupo multiplicativo, y su multiplicación es distributiva respecto a su adición: $A/\mathcal{R}$ es pues, un anillo, llamado *anillo cociente* o, de manera más precisa, *anillo de las clases de restos módulo $\mathcal{R}$* .

En particular, si A es el anillo de los enteros $\mathbb{Z}$ y $\mathcal{R}$ es la congruencia aritmética módulo m , obtendremos el *anillo de las clases de restos módulo m* , llamado también anillo de los enteros módulos m . Hemos dado antes (loc. cit.) las tablas de adición y multiplicación de este anillo en el caso $m = 6$.

Las propiedades generales establecidas, como consecuencia de la distributiva, al final del párrafo precedente son válidas en todo anillo A ; así tendremos la fórmula:

$$\left(\sum_{\lambda=1}^r u_{\lambda}\right) \left(\sum_{\mu=1}^s v_{\mu}\right) = \sum_{\lambda, \mu=1}^{r, s} u_{\lambda} v_{\mu},$$

que implica en particular

$$(a + b)^2 = a^2 + ab + ba + b^2$$

y, si a y b son permutables, en particular si el anillo A es conmutativo,

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Para un exponente n cualquiera, el desarrollo de $(a + b)^n$, donde a, b son dos elementos *permutables* de A , se obtiene por recurrencia y viene dado por la clásica *fórmula del binomio*:

$$(a + b)^n = a^n + na^{n-1}b + \dots + \binom{n}{k} a^{n-k}b^k + \dots + b^n$$

con

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

lo que da como expresión del coeficiente general $\binom{n}{k}$ o C_n^k :

$$\binom{n}{k} = \frac{n(n-1) \dots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Por otra parte, la multiplicación es distributiva respecto a la sustracción:

$$x(a - b) = xa - xb, \quad (a - b)y = ay - by$$

y el 0 es elemento lícito para la multiplicación:

$$0 \cdot x = 0 = x \cdot 0 \quad \forall x \in A.$$

Es decir, que si, en un anillo, *un factor de un producto es nulo, el producto es nulo*. El recíproco no es cierto: *en anillos bastante generales puede muy bien ocurrir que el producto de dos factores no nulos sea igual a cero*.

Sea por ejemplo $\mathcal{F}$ el anillo de las funciones definidas sobre un conjunto X con sus valores en un anillo, por ejemplo en el anillo $\mathbf{R}$ de los números reales. Si A y B son dos partes complementarias de X y si $f, g \in \mathcal{F}$ son dos funciones tales que:

$$f(x) = 0 \quad \forall x \in A \quad \text{y} \quad g(x) = 0 \quad \forall x \in B$$

con $f(x) \neq 0$ para al menos un $x \in B$, $g(x) \neq 0$ para al menos un $x \in A$, tendremos:

$$fg = 0, \quad f \neq 0, \quad g \neq 0.$$

Tomando $X = \mathbf{R}$, $A = \mathbf{R}^+ = \{x; x \geq 0\}$, las funciones $f = \max(x, 0)$; $g = \min(x, 0)$ responden a la cuestión. Se pueden tomar también para f y g las funciones características C_A y C_B de dos conjuntos A y B complementarios en X [$C_A(x) = 0$ para $x \in B$, $C_A(x) = 1$ para $x \in A$].

Igualmente, para $X = N$, las sucesiones

$$\alpha = (1, 0, 1, 0, 1, 0, \dots), \quad \beta = (0, 1, 0, 1, 0, 1, \dots)$$

son tales que

$$\alpha\beta = 0 (\in \mathcal{F}),$$

bien que α y β sean diferentes del cero del anillo $\mathcal{F}$, es decir, de la sucesión $(0, 0, \dots, 0, \dots)$.

Lo mismo en los anillos de enteros módulo m podemos encontrar, si m no es primo, productos que son nulos sin que ningún factor lo sea. Así, designando por $\bar{x}$ la clase módulo m que contiene a x , tenemos

$$\begin{aligned} m = 4, \quad \bar{2} \cdot \bar{2} &= \bar{0}, & (\bar{2} \neq \bar{0}) \\ m = 6, \quad \bar{2} \cdot \bar{3} &= \bar{0} = \bar{4} \cdot \bar{3}, & (\bar{2}, \bar{3}, \bar{4} \neq \bar{0}). \end{aligned}$$

Estas observaciones conducen a las importantes definiciones siguientes:

Definiciones.—En un anillo A (que no suponemos conmutativo) *todo elemento a para el que puede hallarse al menos un elemento $b \neq 0$ tal que*

$$ab = 0$$

se llama divisor de cero a la izquierda; se definen simétricamente los divisores de cero a la derecha. Finalmente, se llama divisor de cero a todo elemento x que lo sea a la izquierda y a la derecha:

$$\exists y, z \in A - \{0\} \quad \text{tales que} \quad xy = zx = 0.$$

El elemento 0 es, según esto, divisor de cero. Pero un divisor de cero a la izquierda, (por ejemplo) se dice *propio* o *verdadero*, cuando no es nulo. Es claro que un anillo A sin verdaderos divisores de cero a la izquierda, tampoco los tiene a la derecha; un anillo así, que se llama *íntegro*, está caracterizado por la propiedad:

$$a \neq 0 \quad \text{y} \quad b \neq 0 \quad \text{implica} \quad ab \neq 0$$

Esto es como decir, en otros términos, que $A^* = A - \{0\}$ es una parte

estable para la multiplicación, o sea, un *subsemigrupo* multiplicativo de A (considerado A como semigrupo multiplicativo). Es importante señalar que en A^* es válida la *regla de simplificación para los productos*, o ley cancelativa. Sea en efecto:

$$ax = bx, \quad \text{donde } a, b, x \in A^*$$

Esta igualdad se escribe:

$$(a - b)x = 0,$$

de donde, puesto que x no es divisor de cero a la derecha,

$$a - b = 0.$$

Se llama *dominio de integridad* un anillo íntegro y conmutativo¹.

En cualquier anillo A , un elemento x se dice *nilpotente* si existe un entero positivo ν tal que $x^\nu = 0$. Un elemento $x \neq 0$ y nilpotente es divisor de cero. En un dominio de integridad no hay otro elemento nilpotente que el 0.

Teorema 1. — *Para que el anillo $\mathbb{Z}/(m)$ de los enteros módulo m sea un dominio de integridad, es necesario y suficiente que m sea un número primo.*

Desde luego, si m no es primo, $m = ab$ con a, b distintos de 1 y de m ; las clases $\bar{a}, \bar{b} \in \mathbb{Z}/(m)$ no son nulas y sin embargo su producto $\bar{a}\bar{b} = \bar{m}$ es la clase nula.

Supongamos ahora, m primo: $m = p$. Si en $\mathbb{Z}/(p)$ es $\bar{a} \cdot \bar{b} = \bar{0}$ y si a y b son dos enteros situados respectivamente en las clases $\bar{a}, \bar{b}$ el producto $ab (\in \bar{a}\bar{b})$ es múltiplo de p ; como p es primo, uno al menos de los números a, b es múltiplo de p , es decir, en $\mathbb{Z}/(p)$ uno al menos de los factores $\bar{a}, \bar{b}$, es igual a $\bar{0}$; por lo tanto $\mathbb{Z}/(p)$ es un dominio de integridad.

Se llama *subanillo* de un anillo B , una parte A de B que sea asimismo anillo respecto de la adición y de la multiplicación de B ; esto exige que A sea:

- 1.º un subgrupo aditivo de B (de donde $A \neq \emptyset$);
- 2.º una parte estable de B para la multiplicación.

Estas dos condiciones necesarias son suficientes, pues, si se cumplen, la multiplicación en A , restricción de la de B es asociativa y distributiva respecto de la adición con A , también restricción de la de B .

El mismo B y el $\{0\}$ son siempre subanillos del B , a los que se califica de *impropios*. Los otros subanillos de B , se llaman *propios*.

Cualquier subanillo de un anillo íntegro es también íntegro.

Ejemplos. — 1. El conjunto de los números pares es un subanillo del anillo

¹ Diversos autores exigen, además, que el anillo tenga elemento unidad. (N. del T.)

de los enteros $\mathbf{Z}$. El anillo $\mathbf{Z}$ es un subanillo del anillo $\mathbf{G}$ de los enteros de Gauss, y también del anillo $\mathbf{Q}$ de los números racionales.

2. Para p primo, el anillo $\mathbf{Z}/(p)$ de los enteros módulo p no tiene ningún subanillo propio pues, como grupo aditivo de orden primo no admite subgrupos propios.

La familia $\mathcal{F}$, de los subanillos de un anillo B es una *familia de Moore*, intersección de la familia de Moore de los subgrupos aditivos y de la familia de Moore de las partes estables para la multiplicación. La clausura de Moore $M \rightarrow \overline{M}$ asociada a esta familia define el *mínimo subanillo* $\overline{M}$ de B que contiene a una parte dada M de B ; se dice que $\overline{M}$ es el *subanillo engendrado por M* . Supongamos en particular que B tiene un elemento unidad e ; éste engendra un subgrupo aditivo $\Gamma = (e)$, finito o infinito (cf. § 5) conjunto de los elementos ne ($n \in \mathbf{Z}$). Pero tenemos:

$$ne \cdot n'e = nn' \cdot e$$

y el subgrupo aditivo Γ engendrado por e , estable para la multiplicación, es también el subanillo engendrado por e ; este subanillo es conmutativo y cualquiera de sus elementos es permutable con todos los elementos de B .

Si A es subanillo de B , se dice también que B es un *superanillo* de A . De manera un poco más general, se dice que un anillo B , es *extensión* de un anillo A si contiene un subanillo A' isomorfo a A , es decir si existe una biyección φ de A sobre A' para la que sea

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \varphi(xy) = \varphi(x) \varphi(y).$$

Dados un anillo B , un subanillo A y un subconjunto cualquiera S de B , la intersección I de los subanillos X de B que contienen a A y a S , es también un subanillo que contiene a A y a S ; I es pues el *mínimo anillo comprendido entre A y B que contiene a S* . Se dice que I es el subanillo obtenido por *adjunción* de S a A , y se escribe:

$$I = A[S].$$

Si $\overline{M}$ indica el subanillo engendrado por un subconjunto M de B , se tiene:

$$A[S] = \overline{A \cup S}$$

y por consiguiente, cuando $S = S_1 \cup S_2$,

$$A[S_1 \cup S_2] = \overline{A \cup S_1 \cup S_2} = \overline{\overline{A \cup S_1} \cup S_2} = A[S_1][S_2]$$

(según una fórmula del cap. I, § 5). De este modo se obtiene el mismo subanillo adjuntando a A la reunión $S_1 \cup S_2$, o adjuntando primero S_1 a A , y luego S_2 al anillo $A[S_1]$ así formado. En particular, se puede reemplazar la adjunción simultánea de n elementos $a_1, a_2, \dots, a_n$ de B por n adjunciones sucesivas de un solo elemento.

El anillo $A[a]$ obtenido cuando se adjunta un solo elemento $a (\in B)$ al anillo A , se llama *extensión simple* de A .

Definiciones. — En un anillo A con elemento unidad e ($e \neq 0$), (según la convención antes hecha) un elemento u se llama *unidad* si es inversible (respecto a e), es decir si existe un elemento u^{-1} de A que satisface las dos igualdades.

$$uu^{-1} = u^{-1}u = e.$$

El elemento u^{-1} es también unidad. Por otra parte el producto $u_1 u_2$ de dos unidades es también unidad, puesto que $(u_1 u_2) (u_2^{-1} u_1^{-1}) = e$. El conjunto U de las unidades del anillo A , es pues, *estable* para la multiplicación y nunca es vacío puesto que contiene a e y $-e$. Por lo tanto es un *grupo multiplicativo* llamado *grupo de las unidades*. Poniendo $A^* = A - \{0\}$ resulta $U \subseteq A^*$ pues 0, elemento lícito para la multiplicación, nunca es inversible.

Ejemplos. — 1. En el anillo $\mathbf{Z}$ de los números enteros, el grupo de las unidades es el grupo $U = \{+1, -1\}$, cíclico del orden 2. En el anillo de los enteros de Gauss, $\mathbf{G}$, la igualdad.

$$(a + bi)(a' + b'i) = 1$$

implica, tomando módulos

$$(a^2 + b^2)(a'^2 + b'^2) = 1$$

de donde $a^2 + b^2 = 1$ que admite en $\mathbf{Z}$ las soluciones $a = \pm 1, b = 0$ y $a = 0, b = \pm 1$. Tenemos pues, $U = \{+1, i, -1, -i\}$ grupo cíclico de orden 4.

2. En el anillo de los números racionales $\mathbf{Q}$, todo elemento no nulo es inversible: tenemos aquí $U = \mathbf{Q}^*$.

Igualmente para el anillo de los números reales, $\mathbf{R}$, y para el anillo de los números complejos, $\mathbf{C}$, se tiene, respectivamente, $U = \mathbf{R}^*, U = \mathbf{C}^*$. Estos casos notables nos llevan a la definición fundamental siguiente.

§ 3. Cuerpos

Se llama *cuerpo* a un anillo K con elemento unidad e ($e \neq 0$), y en el que, además, todo elemento $a \neq 0$ tiene un inverso a^{-1} :

$$aa^{-1} = e = a^{-1}a.$$

Un cuerpo K es pues *un anillo con elemento unidad y en el cual el grupo de las unidades U es $K^* = K - \{0\}$* . Así, K^* es una parte estable respecto a la multiplicación, y por consiguiente, *todo cuerpo es íntegro*.

Inversamente si K es un anillo y $K^* = K - \{0\}$ es grupo multiplicativo (con lo que se sobreentiende que K^* no es vacío, y que es estable para la multiplicación). K es un cuerpo. En efecto el elemento unidad e del grupo K^* es elemento unidad del anillo K (puesto que, además, $e0 = 0 = 0e$) y, por hipótesis, todo elemento $a \neq 0$, pertenece a K^* y posee un inverso.

Otra propiedad característica de un cuerpo es la siguiente:

En un cuerpo K , cualesquiera sean los elementos $a \neq 0$ y b , las ecuaciones

$$(1) \quad ax = b, \quad ya = b$$

tienen, cada una, una solución y sólo una

$$x = a^{-1}b, \quad y = ba^{-1}.$$

Recíprocamente, sea K un anillo, no reducido a $\{0\}$, y tal que para todo $a \neq 0$ y cualquier b , cada una de las ecuaciones (1) admite al menos una solución. Demostremos que K es un cuerpo. Como no es evidente que K^* sea estable para la multiplicación, razonaremos de la manera siguiente. Sea a un elemento particular de K^* . Existe al menos un elemento e de K tal que $ae = a$; para todo elemento r de K existe un elemento m de K tal que $r = ma$, de donde $re = mae = ma = r$; y e es elemento unidad a la derecha; existe igualmente un elemento unidad a izquierda e' y se tiene: $e'e = e = e'$. En fin, para todo elemento $a \neq 0$, existen un elemento a' y un elemento a'' tales que $a'a = e = aa''$ y se tiene $a'aa'' = a'' = a'$; K es, efectivamente, un cuerpo.

Un cuerpo K , es pues, un anillo que tiene al menos dos elementos, y en el que cada una de las igualdades (1) tiene al menos una solución (y entonces esta solución es necesariamente única). Esta proposición puede tomarse, también, como definición de cuerpo.

Un cuerpo cuya multiplicación es conmutativa se llama *conmutativo*, adjetivo que de ordinario se sobreentiende. Cuando no se supone la conmutatividad se prefiere decir que se trata de un *anillo de división*; y *cuerpo oblicuo* significa en principio, cuerpo con multiplicación no conmutativa.

Se demuestra que *todo cuerpo constituido por un número finito de elementos es conmutativo*; este teorema, debido a Wedderburn, será demostrado en cap. X, § 9. Nos limitaremos ahora a dos proposiciones más simples.

Teorema 1. — *Todo anillo íntegro (en particular todo dominio de integridad) con sólo un número finito de elementos, es un cuerpo.*

Sea A un anillo íntegro; $A^* = A - \{0\}$, es como hemos visto, un semigrupo multiplicativo que cumple la regla de simplificación. Y como A^* tiene un número finito de elementos, será un grupo respecto de la multiplicación (cap. II, § 2, teor. 4) y A un cuerpo, como queríamos demostrar.

De este teorema y del teorema 1 de § 2, resulta, que *para todo número primo p , el anillo $\mathbb{Z}/(p)$ de enteros módulo p , que tiene p elementos, es un cuerpo.*

Los cuerpos con sólo un número finito de elementos, cuya existencia hemos establecido, se llaman cuerpos finitos. Su estudio se inicia en Galois: por esta razón, se les llama también *campos de Galois*.

Ejemplos de cuerpos. — 1. Escribamos, para $p = 2$, las tablas de suma y multiplicación del *cuerpo de los enteros módulo 2*, $\{0, 1\}$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Del mismo modo se pueden escribir, para valores pequeños de p , ($p = 3, 5, \dots$) las tablas de adición y multiplicación del campo de Galois $\mathbb{Z}/(p)$.

2. El conjunto de los números racionales $\mathbb{Q}$, el conjunto de los números reales $\mathbb{R}$, el conjunto de los números complejos $\mathbb{C}$, son cuerpos.

3. El conjunto de los números reales de la forma $a + b\sqrt{2}$ en que a, b son dos números *racionales* cualesquiera, es un cuerpo; en efecto $a = a + b\sqrt{2}$ es diferente de cero, cuando a y b no son simultáneamente nulos y entonces a admite el inverso.

$$a^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

El teorema siguiente ofrece un procedimiento fundamental para la construcción de cuerpos.

Teorema 2. — *Todo dominio de integridad D , puede ser sumergido en un cuerpo (en otros términos, existe un cuerpo que es una extensión de D).*

Pongamos $D - \{0\} = S$ y consideremos el conjunto producto $\Pi = D \times S$, es decir el conjunto de los pares (a, b) de elementos de D en los que es $b \neq 0$. Introducimos en Π la multiplicación definida por

$$(a, b)(a', b') = (aa', bb')$$

y la relación $\mathcal{E}$ definida por

$$(a, b) \mathcal{E}(a_1, b_1) \quad \text{si} \quad ab_1 = a_1b.$$

En $\Delta = S \times S$, subconjunto de Π , $\mathcal{E}$ es la equivalencia utilizada para la inmersión del semigrupo abeliano S , en el que vale la regla de simplificación, en el grupo $\Gamma = \Delta/\mathcal{E}$. Pero dos pares cualesquiera de la forma $(0, b)$ verifican la relación $\mathcal{E}$, y $(0, b) \mathcal{E}(x, y)$ implica $xb = 0$, esto es, $x = 0$, puesto que D es un dominio de integridad: $\mathcal{E}$ realiza, pues, una partición de Π en clases disjuntas que son, por una parte los elementos del grupo $\Gamma = \Delta/\mathcal{E}$, por otra parte las clases formadas por los pares $(0, b)$ que llamaremos la *clase cero*, y denotaremos por $\bar{0}$. Designemos por $K = \Gamma \cup \{\bar{0}\} = \Pi/\mathcal{E}$ el conjunto de estas clases. En K , cualquier producto por $\bar{0}$ es igual a $\bar{0}$.

Para hacer de K un cuerpo (conmutativo), es suficiente definir una adición que tenga las propiedades pedidas, y para esto se introduce, por analogía, con la teoría elemental de las fracciones (en las cuales $D = \mathbf{Z}$, anillo de los enteros), la suma de dos pares (a, b) , (a', b') definida en Π por

$$(a, b) + (a', b') = (ab' + ba', bb').$$

Si se reemplaza uno de los dos pares, (a, b) por ejemplo, por un par (a_1, b_1) equivalente a (a, b) módulo $\mathcal{E}$, la suma queda reemplazada por un par equivalente, pues la igualdad $ab_1 = a_1b$ implica

$$(ab' + ba')b_1b' = (a_1b' + b_1a')bb'$$

La relación de equivalencia $\mathcal{E}$ es, pues, compatible con la adición definida en Π lo que permite definir, mediante ésta, una adición en $K = \Pi/\mathcal{E}$.

Las clases representadas por los pares de la forma (am, m) , que se corresponden biyectivamente con los elementos a de D , se adicionan como estos elementos, puesto que tenemos:

$$(am, m) + (a'm', m') = ((a + a')mm', mm').$$

Estas clases particulares forman, pues, un conjunto $\overline{D}$ isomorfo a D , para la adición y la multiplicación.

La adición de K es conmutativa, porque la adición de Π claramente lo es.

Si a, a', a'' son tres elementos de K , representados respectivamente por los pares $(a, b), (a', b'), (a'', b'')$, el par $(ab'b'' + a'b''b + a''bb', bb'b'')$ representa, tanto $(a + a') + a''$ como $a + (a' + a'')$, lo que expresa la igualdad de estas dos expresiones y por consiguiente la *asociatividad* de la adición definida en K . La clase $\overline{0}$ es elemento neutro para la adición; la suma de las clases representadas por (a, b) y por $(-a, b)$ es $\overline{0}$, K es, pues, un grupo abeliano respecto de la adición.

Demostremos finalmente, que en K , la multiplicación es distributiva respecto de la adición. Si ρ es un elemento de K representado por el par (r, s) , el elemento $\rho(a + a')$ estará representado por el par $(r(ab' + ba'), sbb')$, mientras que $\rho a + \rho a'$ está representado por el par

$$(ra, sb) + (ra', sb') = (rs(ab' + ba'), s^2bb')$$

equivalente, módulo $\mathfrak{E}$, al precedente, de donde la igualdad

$$\rho(a + a') = \rho a + \rho a'.$$

En definitiva, K es un cuerpo, llamado *cuerpo de fracciones* (o *cuerpo de cocientes*) del dominio de integridad D . Puesto que $\Gamma = \Delta/\mathfrak{E}$ es un grupo minimal sobre un semigrupo multiplicativo $\overline{S}$ isomorfo a S , será $K = \Pi/\mathfrak{E}$ un cuerpo *minimal* incluyendo a un anillo $\overline{D}$ isomorfo a D .

Para $D = \mathbb{Z}$, el cuerpo obtenido por este procedimiento es el cuerpo de los números racionales $\mathbb{Q}$.

Definición. — Se llama *subcuerpo* de un cuerpo K un subconjunto H de K que también es un cuerpo (respecto a la adición y a la multiplicación de K). Para esto es necesario y suficiente que H sea subgrupo aditivo de K y que $H^* = H - \{0\}$ sea subgrupo multiplicativo de $K^* = K - \{0\}$.

Para que un subanillo S de K sea un subcuerpo, es necesario y suficiente que, para todo elemento $s \in S - \{0\} = S^*$, el inverso s^{-1} de s en K , sea también elemento de S^* .

Si H es un subcuerpo de K , se dice también que K es un *supercuerpo* de H . Se llama *extensión* de un cuerpo K a un cuerpo L que contiene un subcuerpo isomorfo a K . En particular, un supercuerpo es una extensión. Para más precisión, es frecuentemente cómodo, en la teoría de cuerpos, considerar una extensión como el par constituido por el supercuerpo L y el subcuerpo K , y designar esta extensión por la notación $L : K$ o L/K ("*L sobre K*").

Cualquier intersección de subcuerpos de un cuerpo K es subcuerpo de K , y, por consiguiente, *los subcuerpos de K forman una familia de Moore*. La clausura de Moore $X \rightarrow \bar{X}$ correspondiente, asocia a cada parte dada X de K , el menor subcuerpo $\bar{X}$ de K que contiene a X .

Dados un cuerpo K , un subcuerpo H , y un subconjunto cualquiera S de K , la intersección I de los subcuerpos de K que contienen a H y a S es el *menor cuerpo Δ comprendido entre H y K que contiene a S* . Se dice que este subcuerpo se ha obtenido por *adjunción* de S a H (o *adjuntando S a H*), y se escribe:

$$\Delta = H(S).$$

Si $\bar{X}$ designa el subcuerpo engendrado por un subconjunto X de K se tiene

$$H(S) = \overline{H \cup S}$$

y por consiguiente, cuando $S = S_1 \cup S_2$,

$$H(S_1 \cup S_2) = \overline{H \cup S_1 \cup S_2} = \overline{\overline{H \cup S_1} \cup S_2} = H(S_1) (S_2)$$

Se obtiene pues el mismo subcuerpo adjuntando a H la unión $S_1 \cup S_2$, que adjuntando primero S_1 a H , y después S_2 al subcuerpo $H(S_1)$ así formado. En particular se puede reemplazar la adjunción simultánea de n elementos $a_1, a_2, \dots, a_n$ de K por n adjunciones sucesivas de un elemento cada vez. Un cuerpo obtenido adjuntando a H un solo elemento $\alpha (\in K)$ se llama *extensión simple* de H y se indica por $H(\alpha)$.

El elemento unidad e del cuerpo K engendra un subcuerpo $\Pi = \{\overline{e}\}$, evidentemente contenido en cualquier subcuerpo Σ de K , puesto que $e \in \Sigma$. Por esto, Π es la intersección de todos los subcuerpos de K y *no tiene más subcuerpos que él mismo*. Se expresa esta propiedad diciendo que Π es un *cuerpo primo*, o que es el *subcuerpo primo* de K .

El subcuerpo primo Π de K contiene el subanillo $\Gamma = \{ne; n \in \mathbb{Z}\}$ engendrado por el elemento unidad e , anillo íntegro y conmutativo. Si Γ es un subcuerpo, debe ser $\Pi = \Gamma$ y Π es conmutativo; este caso se presenta por ejemplo para el cuerpo $K = \mathbb{Z}/(p)$ de los enteros módulo p ; tendremos aquí $\Gamma = \Pi = K$, y K es primo.

Si el dominio de integridad Γ no es un cuerpo, el conjunto P de los elementos $me(ne)^{-1}$ ($m, n \in \mathbb{Z}, ne \neq 0$), contiene al 0 y con cada elemento su opuesto, ya que $(-m)e \cdot (ne)^{-1}$, es opuesto del antedicho. Además tenemos

$$me \cdot (ne)^{-1} + m'e \cdot (n'e)^{-1} = (mn' + m'n) e \cdot (nn'e)^{-1}$$

(como se ve multiplicando los dos miembros por $ne \cdot n'e$). Por todo ello P es un

grupo aditivo. En cuanto a $P^* = P - \{0\}$ es el conjunto de los elementos $me \cdot (ne)^{-1}$ ($me \neq 0, ne \neq 0$) que es un grupo multiplicativo, luego P es el menor subcuerpo que contiene a e : tenemos pues $P = \Pi$ y, también aquí, Π es conmutativo. Así:

Teorema. — *El subcuerpo primo Π de un cuerpo K cualquiera es conmutativo; si no coincide con el subgrupo aditivo (o el subanillo) $\Gamma = \{ me ; m \in \mathbb{Z} \}$ engendrado por e , es el conjunto de los elementos $me \cdot (ne)^{-1}$ ($m, n \in \mathbb{Z}, ne \neq 0$), cuerpo de fracciones del dominio de integridad Γ .*

El estudio de las propiedades aditivas de los anillos nos va a permitir precisar la distinción entre los dos casos $\Gamma = \Pi$ y $\Gamma \neq \Pi$.

§ 4. Grupo aditivo de un anillo. Característica

Estudiemos el grupo aditivo A_+ de un anillo A y sus subgrupos cíclicos $(x) = \{ \dots, -x, 0, x, 2x, \dots \}$, $x \in A$. Esto nos llevará a la importante noción de *característica*.

Designemos por $\nu(x)$ el orden del grupo cíclico (x) engendrado por x . Este $\nu(x)$ será, o un *entero natural*, o *infinito*. Para que

$$nx = 0 \quad (n \text{ entero} \geq 0)$$

es necesario y suficiente:

si $\nu(x)$ es finito, que n sea múltiplo de $\nu(x)$:

$$n = \lambda \nu(x) \quad (\lambda \text{ entero} \geq 0)$$

si $\nu(x)$ es infinito, que

$$n = 0$$

Distingamos entonces los dos casos siguientes, que se excluyen mutuamente:

I. Existe al menos un entero $m > 0$ tal que se tenga

$$mx = 0 \quad \forall x \in A.$$

Resulta que $\nu(x)$ no es infinito para ningún x ; $\nu(x)$ es necesariamente igual a un divisor de m , y por consiguiente no toma más que un número finito de valores, $\nu_1, \dots, \nu_k$ cuando x recorre A . Existe, pues, un *entero positivo mínimo* N tal que se tenga:

$$Nx = 0 \quad \forall x \in A,$$

Este N no es otro que el m.c.m. de los enteros $\nu_1, \dots, \nu_k$. Cualquier entero positivo m tal que

$$mx = 0 \quad \forall x \in A.$$

Será múltiplo de los ν_i , luego también de N .

Se dice entonces que *el anillo A es de característica no nula, N .*

II. *No existe ningún entero positivo m tal que sea*

$$mx = 0 \quad \forall x \in A$$

Este caso es aquel en que el conjunto de los $\nu(x)$ no está acotado superiormente, sea porque $\nu(x)$ es infinito para al menos un x , sea porque $\nu(x)$ tome una infinidad de valores finitos, o sea, en fin porque se den esas dos circunstancias a la vez.

Entonces, 0 es el único entero positivo o nulo n tal que

$$nx = 0 \quad \forall x \in A.$$

Se dice que *A es de característica nula.*¹

Consideremos el caso de un anillo $\mathcal{R}$ que posea al menos un elemento r no divisor de cero a un lado, a la derecha por ejemplo:

$$ar = 0 \quad \text{implica} \quad a = 0$$

($\mathcal{R}$ no lo suponemos conmutativo). Para todo entero natural n y todo elemento x de $\mathcal{R}$, se tiene:

$$(nx)r = x(nr)$$

luego, si $nr = 0$, $(nx)r = 0$, de donde $nx = 0$.

Entonces si el grupo aditivo (r) es de orden finito $\nu(r)$, se tiene

$$\nu(r)x = 0, \quad \forall x \in \mathcal{R}.$$

El orden $\nu(x)$ de (x) no es infinito; es un divisor de $\nu(r)$, el anillo $\mathcal{R}$ es de característica no nula, $N = \nu(r)$.

¹ Algunos autores dicen que A es de característica infinita, y otros que es un anillo sin característica. (N. del T.)

Por consiguiente, o bien $\mathcal{R}$ es de característica nula, y entonces todos los no divisores de cero a la derecha o a la izquierda engendran grupos cíclicos aditivos infinitos; o bien $\mathcal{R}$ es de característica $N \neq 0$, y entonces todos los no divisores de cero a la derecha o a la izquierda engendran grupos cíclicos aditivos de orden N .

Además si, en el anillo $\mathcal{R}$, se tiene una relación de la forma $nr = 0$ (n número natural), donde r no es divisor de cero a la derecha o a la izquierda, n es nulo si $\mathcal{R}$ es de característica nula; y n es múltiplo de $v(r)$ y, por tanto, de la característica N , si esta no es cero: se puede decir en todo caso, que n es múltiplo de la característica N .

Casos particulares. — 1. Un anillo A con elemento unidad e ($e \neq 0$), está en el caso precedente. En efecto, $ae = 0$ se escribe $a = 0$ luego e no es divisor de cero. Si $v(e)$ es finito, A es de característica $N = v(e) \neq 0$; si no, A es de característica nula.

2. Sea A un anillo íntegro y no reducido al cero: $A \neq \{0\}$.

Lo que precede se aplica, todo elemento no nulo desempeña el papel de r . Todos los grupos cíclicos aditivos (x) , distintos de (0) , tienen el mismo orden, infinito si la característica es nula, igual a la característica N si ésta es diferente de cero.

Además, siendo A íntegro, la característica es un número primo p . En efecto, la característica N es diferente de 1, puesto que, por hipótesis, existe en A al menos un elemento $x \neq 0$. Si fuese

$$N = nn' \quad (n \neq 1, n' \neq 1),$$

los factores n, n' serían inferiores a N , y para todo elemento $a \neq 0$ de A , tendríamos:

$$na \neq 0, \quad n'a \neq 0,$$

de donde

$$(na)(n'a) \neq 0,$$

lo que es contradictorio, puesto que

$$(na)(n'a) = nn'a^2 = Na^2 = 0.$$

Por lo tanto la característica de un anillo íntegro (en particular de un cuerpo, o de un dominio de integridad), o bien es nula, o bien es un número primo p . Esto enseña que no podremos, en cualquier grupo aditivo abeliano A_+ , definir una multiplicación asociativa y distributiva respecto a la adición, que

haga de A_+ un anillo íntegro A : Para poderlo hacer es necesario que A_+ sea, o bien un grupo sin torsión, o bien un grupo con torsión en el que el orden de todos los elementos sea un mismo número primo p .

En un anillo A , de característica p ($p \neq 0$ y primo), con elemento unidad e , el subgrupo aditivo $(e) = \{0, e, \dots, (p-1)e\}$ engendrado por e , es un subanillo conmutativo Γ , isomorfo a $\mathbf{Z}/(p)$ cuerpo de los enteros módulo p : Γ es, pues, un cuerpo y como, por construcción, no admite subanillos propios, no tiene, *a priori*, subcuerpos propios y todo cuerpo eventual contenido en A contiene a e , y por ende a Γ . Así todo anillo A de característica p (p primo) con elemento unidad e , contiene a un subcuerpo mínimo $\Gamma = \{0, e, \dots, (p-1)e\}$, isomorfo al cuerpo de los enteros módulo p .

En particular, para un cuerpo K de característica p , Γ no es otra cosa que el subcuerpo primo Π , éste tiene, pues, p elementos y es isomorfo al cuerpo de los enteros módulo p , $\mathbf{Z}/(p)$.

Para un cuerpo K de característica nula, el grupo aditivo $\Gamma = (e)$ es infinito, es isomorfo a $\mathbf{Z}$ (como grupo aditivo y como anillo) y el subcuerpo primo Π de K ,

$$\Pi = \{ me \cdot (ne)^{-1}; m, n \in \mathbf{Z}, ne \neq 0 \text{ donde } n \neq 0 \}$$

es isomorfo al cuerpo de los racionales $\mathbf{Q}$.

Para los anillos conmutativos de característica p ($p \neq 0$ primo), incluyendo visiblemente el cuerpo $\mathbf{Z}/(p)$ de los enteros módulo p , se obtienen notables reglas de cálculo. En el desarrollo de $(x+a)^p$,

$$(x+a)^p = x^p + px^{p-1}a + \dots + \binom{p}{k} x^{p-k} a^k + \dots + a^p,$$

el entero

$$\binom{p}{k} = C_p^k = \frac{p(p-1) \dots (p-k+1)}{k!}$$

es, para $k = 1, 2, \dots, p-1$, igual a un múltiplo de p (cap. II, § 6). Se tiene pues

$$\binom{p}{k} x^{p-k} a^k = 0, \quad (k = 1, \dots, p-1),$$

y por consiguiente

$$(x+a)^p = x^p + a^p$$

Sustituyendo x por $x - a$, se obtiene

$$x^p = (x - a)^p + a^p,$$

es decir

$$(x - a)^p = x^p - a^p$$

Estas fórmulas implican sucesivamente

$$\begin{aligned} (a_1 + \dots + a_r)^p &= a_1^p + \dots + a_r^p, \\ (x + a)^{p^f} &= x^{p^f} + a^{p^f}, \\ (x - a)^{p^f} &= x^{p^f} - a^{p^f}, \quad (f = 1, 2, \dots). \end{aligned}$$

Suponiendo ahora que A posee un elemento unidad e y tomando

$$a_1 = a_2 = \dots = a_r = e$$

resulta, escribiendo r , en vez de re ($e \in A$),

$$r^p = r \quad (r \in A),$$

Esta relación es válida, en particular, para el cuerpo de los enteros módulo p : volviendo al anillo de los enteros ≥ 0 , $\mathbf{Z}$ se obtiene:

$$x^p \equiv x \pmod{p}, \quad \forall x \in \mathbf{Z}$$

(teorema de Fermat)

§ 5. Anillos de series formales y anillos de polinomios sobre un anillo conmutativo

Consideremos un subanillo A de un anillo conmutativo B con elemento unidad e ; suponemos que e pertenece también a A , y nos proponemos estudiar una extensión simple $A[\alpha]$ de A ($\alpha \in B$, $\alpha \notin A$).

El anillo $A[\alpha]$ contiene, con α , sus potencias, y también todas las sumas

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = \sum_{i=0}^n a_i\alpha^i, \quad a_i \in A, \quad n \text{ entero } \geq 0$$

(conviniendo en poner $a^0 = e$). Una suma tal, donde supondremos $a_n \neq 0$, se llama *expresión polinómica de grado n en a , de coeficientes en A* . Suponiendo B conmutativo, el conjunto P de estas expresiones polinómicas es un subanillo de B , contenido en $A[a]$. Pero, por otra parte P incluye a A , conjunto de expresiones polinómicas de grado 0, y también contiene a $0 + ea = a$; tenemos, pues, $A[a] \subseteq P$ y por consiguiente la igualdad:

$$A[a] = P.$$

Así, con las hipótesis hechas (B anillo conmutativo, con elemento unidad e contenido en el subanillo A), la extensión simple $A[a]$ es el conjunto P de las expresiones polinómicas

$$\sum_{i=0}^n a_i a^i, \quad (a_i \in A)$$

Ejemplos. — 1. Tomemos como anillo B el cuerpo de los números complejos $\mathbf{C}$, como anillo A el anillo de los enteros $\mathbf{Z}$, como elemento a el número i . El anillo $A[a] = \mathbf{Z}(i)$ es el conjunto de las expresiones polinómicas $a_0 + a_1 i + \dots + a_n i^n$; pero como i verifica la igualdad $i^2 + 1 = 0$, cada una de estas expresiones puede escribirse en la forma $a + bi$, con $a, b \in \mathbf{Z}$: el anillo $\mathbf{Z}(i)$ es el anillo de los enteros de Gauss $\mathbf{G}$.

2. Consideremos el anillo B de las funciones:

$$f \quad r \rightarrow f(r)$$

definidas sobre el cuerpo de los números reales $\mathbf{R}$ y tomando sus valores en $\mathbf{R}$. B es una extensión de $\mathbf{R}$, puesto que $\mathbf{R}$ es isomorfo al subanillo A de B formado por las “constantes”:

$$\gamma \quad r \rightarrow c (\in \mathbf{R}) \quad \forall r \in \mathbf{R}.$$

Tomemos para a la función definida por la aplicación idéntica:

$$\alpha \quad r \rightarrow r \quad \forall r \in \mathbf{R}$$

(se advierte que el anillo B tiene como elemento unidad la constante 1, y no la función α). El anillo $A[a]$ es el conjunto de las funciones

$$a_0 + a_1 a + \dots + a_n a^n \quad r \rightarrow a_0 + a_1 r + \dots + a_n r^n$$

$(a_i \in \mathbf{R})$ llamadas *funciones polinómicas* sobre el cuerpo de los números reales $\mathbf{R}$. Según las propiedades elementales de estas funciones, $a_0 + a_1\alpha + \dots + a_n\alpha^n$ coincide con la constante 0 cuando todos los a_i son nulos, y sólo en ese caso.

Nota. — Si se consideran un cuerpo conmutativo K , un subcuerpo H y un elemento α de K no perteneciente a H , el subcuerpo $H(\alpha)$, extensión simple de H , es el subcuerpo engendrado por el anillo $H[\alpha]$, es decir, el conjunto de las *expresiones racionales*:

$$\frac{a_0 + a_1\alpha + \dots + a_r\alpha^r}{b_0 + b_1\alpha + \dots + b_s\alpha^s} \quad (a_i, b_i \in H)$$

cociente de una expresión polinómica cualquiera

$$\sum_{i=0}^r a_i\alpha^i \in H[\alpha]$$

por una expresión polinómica *no nula*

$$\sum_{j=0}^s b_j\alpha^j \in H[\alpha] - \{0\}.$$

Demos ahora la definición algebraica del anillo S de las series formales y del anillo P de los polinomios en x sobre un anillo dado A , que no suponemos necesariamente conmutativo.

Consideremos el conjunto S de las sucesiones

$$\alpha = \{a_0, a_1, \dots, a_n, \dots\} = \{a_n\}, \quad a_n \in A.$$

Una sucesión tal es una aplicación del conjunto $N_0 = \{0, 1, \dots, n, \dots\}$ en A ; dos sucesiones $\alpha = \{a_n\}$, $\beta = \{b_n\}$ son, pues, *iguales* si $a_n = b_n$ para todo $n \in N_0$ y sólo en este caso. Introduciremos en S una *suma término a término*: la sucesión $\{a_n\} + \{b_n\}$ será, por definición, la sucesión $\{a_n + b_n\}$.

Después definiremos en S una multiplicación, diferente de la considerada anteriormente, que era la multiplicación término a término (§ 2, ej. 2). Para evitar toda confusión, y destacar la analogía con el cálculo de series enteras practicado en Análisis, daremos a los elementos de S el nombre de *series formales*.

El producto $\alpha\beta$ de dos series formales $\alpha = \{a_n\}$, $\beta = \{b_n\}$ será por definición, la serie formal $\tilde{\omega} = \{p_n\}$ cuyos *coeficientes* están dados así:

$$(1) \quad \begin{cases} p_0 = a_0 b_0 \\ p_1 = a_0 b_1 + a_1 b_0 \\ \dots\dots\dots \\ p_n = \sum_{\lambda+\mu=n} a_\lambda b_\mu \\ \dots\dots\dots \end{cases}$$

El conjunto S de las series formales con coeficientes en A , al que se dan esta adición y esta multiplicación, tiene las propiedades siguientes:

1.º S es grupo abeliano respecto a la adición.

2.º La multiplicación de S es asociativa, pues, dadas tres series formales $\alpha = \{a_n\}$, $\beta = \{b_n\}$, $\gamma = \{c_n\}$, el coeficiente general r_n de la serie $\rho = (\alpha\beta)\gamma$ y el coeficiente general r'_n de la serie $\rho' = \alpha(\beta\gamma)$ tienen ambos por expresión

$$\sum_{\lambda+\mu+\nu=n} a_\lambda b_\mu c_\nu.$$

3.º Si el anillo A es conmutativo, la multiplicación de S es conmutativa.

4.º La multiplicación de S es distributiva respecto de la adición puesto que el coeficiente general de la serie $(\alpha + \alpha')\beta$ es

$$\sum_{\lambda+\mu=n} (a_\lambda + a'_\lambda) b_\mu = \sum_{\lambda+\mu=n} a_\lambda b_\mu + \sum_{\lambda+\mu=n} a'_\lambda b_\mu,$$

y este es, visiblemente, el coeficiente general de la serie $\alpha\beta + \alpha'\beta$ (vale un razonamiento análogo para la ley distributiva a la izquierda).

S es pues, un anillo llamado *anillo de las series formales sobre el anillo A* .

El conjunto de las *constantes*, es decir, de las series formales

$$\{a_0, 0, \dots, 0, \dots\} \quad (a_n = 0 \quad \forall n \geq 1)$$

es un subanillo $\overline{A}$ de S , isomorfo a A ; S es, pues, una extensión del anillo A ; en lo sucesivo identificaremos A y $\overline{A}$.

Es cómodo utilizar, según el uso, las notaciones siguientes.

Consideremos un *semigrupo multiplicativo monógeno*

$$\Delta = \{x, x^2, \dots, x^n, \dots\}$$

libre, es decir, tal que $\lambda \neq \mu$ implica $x^\lambda \neq x^\mu$, y las sumas formales

$$\alpha(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \dots + a_n x^n + \dots$$

donde $a_n \in A$ y, por convención, $a_0 x^0 = a_0$. Dos de esas sumas:

$$\sum_{n=0}^{\infty} a_n x^n, \quad \sum_{n=0}^{\infty} b_n x^n,$$

serán, por definición, *iguales si, y sólo si, es $a_n = b_n$ para todo n* ; esto lo traduciremos en dar al generador x de Δ el nombre de *indeterminada* (sobre el anillo A). Asociando a

$$\alpha(x) = \sum_{n=0}^{\infty} a_n x^n$$

con la serie formal $\{a_n\}$, definiremos una aplicación biyectiva entre el conjunto $\overline{S}$ de las sumas formales y el conjunto S de las series formales, lo que nos permite definir en $\overline{S}$ una adición y una multiplicación que le constituyen en un anillo isomorfo al S :

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n, \\ \left(\sum_{n=0}^{\infty} a_n x^n \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) &= \sum_{n=0}^{\infty} p_n x^n, \end{aligned}$$

con

$$p_n = \sum_{\lambda + \mu = n} a_\lambda b_\mu.$$

Haciendo abstracción de las cuestiones de convergencia, y considerando, incluso cuando A no es conmutativo, que *la indeterminada x es permutable con cada elemento de A* , esta adición y esta multiplicación no difieren de las que se han considerado en Análisis para las series enteras de una variable. Convendremos para lo sucesivo, en identificar S y $\overline{S}$.

Nota. — Cuando el anillo A posee un elemento unidad e , se puede tomar para indeterminada la serie formal

$$x = \{ 0, e, 0, \dots, 0, \dots \}$$

Esta serie engendra, en efecto, un semigrupo multiplicativo monógeno infinito, pues se tiene:

$$x^n = \{ 0, 0, \dots, 0, e, 0, \dots \}$$

donde e ocupa el lugar de orden $n + 1$. Convengamos por otra parte, en identificar A y $\bar{A}$, es decir $a_n \in A$ con la serie $\{ a_n, 0, \dots, 0, \dots \}$; tenemos

$$a_n x^n = \{ 0, 0, \dots, 0, a_n, 0, \dots \}.$$

En fin, dada una familia de series $\alpha^{(k)} = \{ a_n^{(k)} \}$, ($k = 0, 1, \dots, m, \dots$) tal, que para cada índice n exista solamente un número finito de valores de k para los cuales $a_n^{(k)}$ es diferente de 0, designemos por s_n la suma (en A) de estos $a_n^{(k)} \neq 0$; diremos que la serie $\sigma = \{ s_n \}$ es por definición la suma de las series $\alpha^{(k)}$ y escribiremos

$$\sigma = \sum_k \alpha^{(k)}.$$

Se ve que estas definiciones permiten dar un sentido preciso a la escritura simbólica introducida anteriormente:

$$\{ a_0, a_1, \dots, a_n, \dots \} = \sum_{n=0}^{\infty} a_n x^n.$$

Desde luego, cuando A no tenga elemento unidad, la indeterminada x no podrá ser considerada como un elemento del anillo S de las series formales.

En cualquier caso, el anillo de las series formales en x con coeficientes de A será designado por la notación $A[[x]]$.

Una serie formal en la que sólo el coeficiente a_n es diferente de cero, se llama *monomio* de grado n , y se escribe $a_n x^n$. Aplicada a dos monomios, la regla que define la multiplicación da

$$(a_m x^m) (a_r x^r) = a_m a_r x^{m+r},$$

lo que pone en evidencia la permutabilidad de la indeterminada x con los elementos de A .

Una serie formal en la cual hay solamente un número finito (≥ 0) de coeficientes a_n diferentes de cero se llama *polinomio*. El mayor índice m , para el que a_m es diferente de cero, es el *grado* del polinomio (se advertirá que el grado del polinomio cero no está definido), el monomio a_mx^m es el término *director*, o *principal*, del polinomio; su coeficiente, a_m , es el *coeficiente director* (o *principal*) del polinomio. Para designar un polinomio de grado m , se emplea generalmente una de las notaciones:

$$f(x) = \sum_{i=0}^m a_i x^i = a_0 + a_1 x + \dots + a_m x^m.$$

Los polinomios en x de coeficientes en A forman un subanillo P del anillo de las series formales S . P contiene como subanillo a A (identificado al anillo de constantes). En el anillo P , todo polinomio es la suma de los monomios $a_i x^i$ que figuran en él; y el producto de polinomios coincide con el calculado como producto de sumas de monomios, teniendo en cuenta la propiedad distributiva y la regla de multiplicación de dos monomios.

Si el anillo A tiene un elemento unidad e , x es un polinomio (con $a_1 = e$ y $a_i = 0$ para $i \neq 1$, poniendo $ex = x$); entonces el anillo de los polinomios P es, en S , la extensión simple de A obtenida por adjunción de x ; se escribe, pues,

$$P = A[x]$$

y es costumbre conservar esta notación cuando A no tiene elemento unidad (constituye así un abuso de escritura, pero no trae consigo inconvenientes reales).

Nota. — Dado un anillo A , puede ser útil considerar simultáneamente diferentes indeterminadas, $x, y, \dots$ y los anillos $A[[x]], A[[y]], \dots$; estos anillos son isomorfos entre sí, puesto que todos son isomorfos al anillo S de las series formales consideradas como sucesiones de sus coeficientes. Los anillos de polinomios $A[x], A[y], \dots$ también son isomorfos. Se resumen estas propiedades diciendo que, dado el anillo A , el anillo $A[[x]]$ o el anillo $A[x]$ están *definidos a menos de un isomorfismo*, o *salvo isomorfismos*.

Teorema 1. — Si el anillo A es íntegro, el anillo de las series formales $A[[x]]$ también lo es.¹

Sean

$$\alpha = \sum_{i=0}^{\infty} a_i x^i, \quad \beta = \sum_{j=0}^{\infty} b_j x^j$$

¹ Este teorema y el siguiente son ejemplos de los que en Álgebra se llaman *teoremas de transferencia*. En ellos se expresa que determinada propiedad, válida para un conjunto A con

dos series formales no nulas; designemos por λ el menor índice tal, que a_λ sea distinto de cero, y por μ el menor índice tal que b_μ no sea nulo. El coeficiente de índice $\lambda + \mu$ en la serie producto $\alpha\beta$ es $a_\lambda b_\mu \neq 0$, y, por consiguiente, $\alpha\beta$ es distinto de la serie nula.

Corolario. — Si A es un dominio de integridad, $A[[x]]$ también lo es.

Efectivamente, porque hemos visto que la conmutatividad de la multiplicación se conserva cuando se pasa A a $A[[x]]$.

Teorema 2. — El producto de dos polinomios:

$$f = \sum_{i=0}^m a_i x^i, \quad g = \sum_{j=0}^n b_j x^j$$

del anillo $A[x]$, de grados m, n , respectivamente, es, o bien el polinomio nulo, o bien un polinomio de grado no superior a $m + n$.

Si A es íntegro, el producto fg es de grado $m + n$, y $A[x]$ también es un anillo íntegro. Si A es un dominio de integridad, también lo es $A[x]$.

En el producto fg , todos los coeficientes de índice superior a $m + n$ son nulos; el coeficiente de x^{m+n} es $a_m b_n$ y tendremos $a_m \neq 0$ y $b_n \neq 0$. De esto se deduce el teorema.

Si el anillo A es íntegro, el producto de dos polinomios que no sean constantes no es constante; por consecuencia, las unidades del anillo $A[x]$ son las constantes u que sean unidades de A ; si A es un cuerpo K , éstas son todos los elementos no nulos de K .

Nota. — La característica de un anillo A es también la de los anillos $A[x]$ y $A[[x]]$.

Estos mismos principios permiten definir, a partir de un anillo A el anillo de las series formales $S_r = A[[x_1, x_2, \dots, x_r]]$ y el anillo de los polinomios $P_r = A[x_1, x_2, \dots, x_r]$ en r indeterminadas $x_1, \dots, x_r$, siendo r un entero positivo cualquiera. Limitémonos para simplificar la escritura al caso $r = 2$ y designemos las dos indeterminadas por x e y .

Consideremos un semigrupo multiplicativo engendrado por x e y ,

$$\Delta_2 = \{x, y, \dots, x^m y^n, \dots\}$$

y libre, es decir tal que la igualdad $x^\lambda y^\mu = x^{\lambda'} y^{\mu'}$ exija $\lambda = \lambda', \mu = \mu'$. Con-

cierta estructura algebraica, es también válida para una extensión A' de A , que se construye a partir de A con determinado procedimiento.

sideremos de otra parte las series formales

$$a(x, y) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} a_{m,n} x^m y^n, \quad (a_{m,n} \in A),$$

donde por convención $a_0 x^0 y^0 = a_0$, $a_{m,0} x^m y^0 = a_{m,0} x^m$, y $a_{0,n} x^0 y^n = a_{0,n} y^n$.

Dos de tales series, de coeficientes $a_{m,n}$, $b_{m,n}$ son, por definición, iguales si $a_{m,n} = b_{m,n}$ cualesquiera sean m y n . La adición de series formales se realiza término a término, y la multiplicación se define por la fórmula:

$$\left(\sum_{m=0}^{\infty} \sum_{n=0}^{\infty} a_{m,n} x^m y^n \right) \cdot \left(\sum_{m=0}^{\infty} \sum_{n=0}^{\infty} b_{m,n} x^m y^n \right) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} p_{m,n} x^m y^n$$

donde

$$p_{m,n} = \sum_{\mu+\mu'=m, \nu+\nu'=n} a_{\mu,\nu} b_{\mu',\nu'}.$$

El conjunto S_2 de las series formales $a(x, y)$ con esta adición y esta multiplicación es un anillo, extensión de A y también de $A[[x]]$, pues las series formales sin términos en y , es decir, en las que $a_{m,n} = 0$ para todo $n \neq 0$, constituyen un subanillo isomorfo a $A[[x]]$, al que convendremos en identificar con éste. Del mismo modo S_2 contiene a $A[[y]]$ como subanillo. Escribiremos, para lo sucesivo, $S_2 = A[[x, y]]$.

Llamamos *monomio* a una serie formal en la que sólo un coeficiente $a_{m,n}$ es diferente de cero, y lo escribiremos $a_{m,n} x^m y^n$; el grado de este monomio es $m + n$. Aplicada a dos monomios, la regla para la multiplicación da:

$$a_{m,n} x^m y^n \cdot b_{r,s} x^r y^s = a_{m,n} b_{r,s} \cdot x^{m+r} y^{n+s}.$$

Esto implica como vemos, la *permutabilidad* de las indeterminadas x , y entre ellas y con los elementos de A .

Llamamos polinomio en x , y , a una serie formal $a(x, y)$ en la que hay sólo un número finito (≥ 0) de coeficientes no nulos; su grado es el máximo grado de los monomios que en él figuran efectivamente (es decir, con coeficiente no nulo). Los polinomios así definidos forman un subanillo $P_2 = A[x, y]$ de S_2 , en el que está contenido A como subanillo. En este anillo P_2 , todo polinomio es, como en el caso de una indeterminada, la suma de los monomios que lo componen, y el producto de dos polinomios coincide con el producto que se obtiene si se les considera como sumas de monomios (para el que se deben aplicar la propiedad distributiva y la regla de multiplicación de monomios).

Finalmente el anillo $A[x, y]$ es el mismo $A[x][y]$ que se obtendría formando el anillo de polinomios en y con coeficientes en $A[x]$.

En el anillo $A[x_1, x_2, \dots, x_r]$ de polinomios en $x_1, x_2, \dots, x_r$ sobre A , es decir, con coeficientes en A , se llama *polinomio homogéneo*, o *forma* de grado n , a un polinomio en el que todos los monomios con coeficientes distinto de cero, tienen el grado n . El producto de dos formas es una forma y, si el producto no es nulo, su grado es la suma de los grados de los factores.

Un polinomio cualquiera de grado n es la suma de partes homogéneas de grados respectivos $0, 1, 2, \dots, n$ (pudiendo ser algunas nulas). Resulta, por ello, que el producto de un polinomio f de grado m por un polinomio g de grado n es un polinomio, de grado a lo más $m + n$. Si A es un anillo íntegro el grado del producto es exactamente $m + n$. Es suficiente, para probarlo, ordenar los monomios que figuran en cada polinomio poniendo:

$$x_1^{a_1} x_2^{a_2} \dots x_r^{a_r} < x_1^{\beta_1} x_2^{\beta_2} \dots x_r^{\beta_r}$$

si

$$a_1 + a_2 + \dots + a_r < \beta_1 + \beta_2 + \dots + \beta_r$$

o si

$$a_1 + a_2 + \dots + a_r = \beta_1 + \beta_2 + \dots + \beta_r, a_r = \beta_r, \dots, a_{k+1} = \beta_{k+1}, a_k < \beta_k$$

($1 \leq k \leq r$). Esta relación de orden es respetada por la multiplicación. El último monomio del producto fg , es el producto de los últimos monomios de f y g , lo que establece el resultado. Por lo tanto, si A es íntegro, el anillo $A[x_1, x_2, \dots, x_r]$ lo es también.

Un razonamiento análogo hecho sobre los primeros monomios con coeficientes no nulos que figuren en las series formales demuestra que, si A es íntegro, $A[[x_1, x_2, \dots, x_r]]$ también lo es.

Si A es un dominio de integridad, el anillo de polinomios $A[x_1, x_2, \dots, x_r] = P_r$ lo es también, y su cuerpo de cocientes K_r , se llama *cuerpo de las fracciones racionales* en $x_1, x_2, \dots, x_r$ sobre el anillo A , y se denota así:

$$K_r = A(x_1, \dots, x_r).$$

Si Δ es el cuerpo de las fracciones de A , es claro que también se tiene:

$$K_r = \Delta(x_1, \dots, x_r).$$

Consideremos, con el anillo, A , un superanillo B de A , que puede coincidir con A , y que no suponemos conmutativo. Sea:

$$f(x_1, \dots, x_r) = \sum a_{\alpha_1, \dots, \alpha_r} x_1^{\alpha_1} \dots x_r^{\alpha_r}$$

un polinomio del anillo $P_r = A[x_1, \dots, x_r]$.

Si $b_1, b_2, \dots, b_r$ son r elementos (distintos o no) de B , resulta cómodo llamar *punto*, y designar por b , al elemento $b = (b_1, \dots, b_r)$ del conjunto producto B^r . El elemento

$$\varphi = \sum a_{\alpha_1, \dots, \alpha_r} b_1^{\alpha_1} \dots b_r^{\alpha_r}$$

del anillo B obtenido reemplazando x_i por b_i ($i = 1, 2, \dots, r$) en $f(x_1, x_2, \dots, x_r)$ se llama *valor* del polinomio f en el punto b y se designa por $f(b_1, \dots, b_r)$.

Si g es otro polinomio de P_r y ponemos $f + g = s$, tenemos

$$s(b_1, \dots, b_r) = f(b_1, \dots, b_r) + g(b_1, \dots, b_r);$$

el valor de la suma de dos polinomios, f, g , en un punto b es la suma de los valores de f y de g en ese punto.

Si ahora consideramos el polinomio $p = fg$, producto de los polinomios dados, no es cierto en general que su valor en el punto b sea el producto de los valores de f y de g en ese punto. En efecto, el cálculo de p a partir de f y g se basa en el hecho de ser permutables las indeterminadas entre sí y con los coeficientes de f , elementos de A . Ahora bien, los elementos b_i del anillo B por los cuales se reemplazan las x_i no poseen, en general, esa permutabilidad.

Por ejemplo, el producto de polinomios $f = x - a_1, g = x - a_2$ ($a_1, a_2 \in A$) es el polinomio:

$$p(x) = (x - a_1)(x - a_2) = x^2 - (a_1 + a_2)x + a_1a_2$$

y tenemos

$$p(a_1) = a_1^2 - (a_1 + a_2)a_1 + a_1a_2 = a_1a_2 - a_2a_1$$

y, por consiguiente, *en un anillo A no conmutativo, a_1 no anula al polinomio $p(x) = (x - a_1)(x - a_2)$, salvo cuando a_1 y a_2 sean permutables.*

Si, por el contrario, los elementos b_i considerados antes, en el anillo B , son permutables entre sí y con cualquier elemento de A , en particular, si el anillo B es conmutativo, la igualdad:

$$p(x_1, \dots, x_r) = f(x_1, \dots, x_r) g(x_1, \dots, x_r)$$

entre polinomios de $A[x_1, \dots, x_r]$; implica:

$$p(b_1, \dots, b_r) = f(b_1, \dots, b_r) g(b_1, \dots, b_r)$$

y, por consiguiente, toda relación entre polinomios del anillo $A[x_1, \dots, x_r]$ resultado de adiciones y multiplicaciones combinadas, permanece cierta cuando se reemplazan las indeterminadas x_i por los antedichos elementos b_i (principio de sustitución).

El hecho de no cumplirse el principio de sustitución sin hipótesis convenientes de permutabilidad entraña, para las propiedades de los anillos de polinomios y las ecuaciones algebraicas, diferencias importantes entre el caso conmutativo y el caso no conmutativo; más adelante tendremos ocasión de insistir sobre esto.

Dado ahora un polinomio fijo $f \in P_r$, asociemos a cada punto b de B^r el valor $\nu = f(b_1, \dots, b_r)$ que toma f en ese punto. Definimos de este modo, a partir de f , una aplicación de B^r en B :

$$f^* \quad b \rightarrow \nu$$

llamada *función polinómica*, o *función polinomio*.

Esta función polinomio no debe ser confundida con el polinomio en sí. En efecto, es bien sabido que, si A y B coinciden con el cuerpo de los números reales $\mathbf{R}$, un polinomio $f(x) \in \mathbf{R}[x]$ está perfectamente caracterizada por la función polinomio asociada f^* (es decir $f^* = g^*$ sólo se cumple para $f = g$); pero existen anillos en los cuales desaparece esta propiedad. Tomemos por ejemplo:

$$A = B = \mathbf{Z}/(2) = \{\bar{0}, \bar{1}\}.$$

Para cualquiera de los polinomios, $x, x^2, \dots, x^n, \dots \in A[x]$, la función correspondiente es la aplicación idéntica de A sobre sí mismo; y todavía, cualquier polinomio no nulo $x^m - x^n$ ($m \neq n$) toma el valor de $\bar{0}$ para todo valor de x en el anillo A . Este importante fenómeno, es la razón de que hayamos introducido los polinomios con un método independiente de la noción de función.

Suponiendo el anillo B conmutativo, consideremos la aplicación $f \rightarrow f^*$, que asocia a cada polinomio f de $A[x_1, \dots, x_r]$ la función polinómica f^* . A los polinomios $s = f + g$ y $p = fg$ corresponden respectivamente, según el principio de sustitución, la suma $f^* + g^*$ y el producto f^*g^* :

$$(f + g)^* = f^* + g^*, \quad (fg)^* = f^*g^*,$$

y por consiguiente, en el caso conmutativo, la aplicación $f \rightarrow f^*$ respeta la adición y la multiplicación.

Sea A un anillo cualquiera (al que no suponemos conmutativo, ni íntegro, ni con elemento unidad). Nos proponemos definir en el anillo de los polinomios $P_1 = A[x]$ una *división con resto generalizada*.

Teorema 3. — Si el coeficiente director, a , de un polinomio de grado m , $f \in A[x]$, es permutable con cada uno de los otros coeficientes de f , existe, para todo polinomio p , de grado n , del anillo $A[x]$, al menos un par de polinomios q y r de este anillo verificando la igualdad

$$a^k p(x) = f(x) q(x) + r(x)$$

con ¹

$$k = \max(0, n - m + 1)$$

y

$$r = 0 \quad \text{o} \quad \text{grado de } r < m.$$

Si, además, a no es divisor de cero a la izquierda en el anillo A , el par (q, r) es único.

La determinación de los polinomios q y r es la *división generalizada a la derecha* de p por f ; q es el cociente a la derecha, r el resto a la derecha.

Si se tiene $n \leq m - 1$, k es nulo, los polinomios $q = 0$, $r = p$, responden a la cuestión.

Para $n \geq m - 1$, tenemos $k = n - m + 1$; siendo cierto el teorema para $n = m - 1$, lo demostraremos por recurrencia para n , suponiéndolo verdadero para todo polinomio de grado inferior a n ($n > m - 1$).

Sea b el coeficiente director de p . En el polinomio:

$$p_1(x) = ap(x) - f(x) \cdot bx^{n-m}$$

el coeficiente de x^n es nulo; p_1 es, pues, de grado $n_1 < n$ y existe, según la hipótesis de recurrencia, un par de polinomios q_1, r_1 de $A[x]$ que cumplen la igualdad

$$a^{k_1} p_1(x) = f(x) q_1(x) + r_1(x),$$

con

$$k_1 = \max(0, n_1 - m + 1) < n - m + 1$$

y

$$r_1 = 0 \quad \text{o} \quad \text{grado de } r_1 < m.$$

Tenemos pues

$$(2) \quad a^{1+k_1} p(x) = f(x) q_1(x) + a^{k_1} f(x) bx^{n-m} + r_1(x).$$

¹ Para $k = 0$, convenimos en poner $a^0 p(x) = p(x)$.

Pero, siendo a permutable con cada coeficiente de $f(x)$, tenemos

$$a^{k_1}f(x) = f(x)a^{k_1}$$

y, multiplicando los dos miembros de (2) por a^{n-m-k_1} , vemos que los polinomios:

$$\begin{aligned} q(x) &= a^{n-m}bx^{n-m} + a^{n-m-k_1}q_1(x), \\ r(x) &= a^{n-m-k_1}r_1(x) \end{aligned}$$

responden a la cuestión.

Si otro par de polinomios q_1, r_1 tiene las mismas propiedades, resulta inmediatamente

$$f(q - q_1) + r - r_1 = 0$$

Si el polinomio $q - q_1$ no fuese nulo, tendríamos, designando por cx^λ su término director ($\lambda \geq 0$, $c \neq 0$), y observando que $r - r_1$, si no es nulo, tiene un grado inferior a m ,

$$ac = 0,$$

lo que es imposible cuando a no es divisor de cero a la izquierda. Se tiene, pues, necesariamente, en este caso, $q_1 = q$ y, por consiguiente, $r_1 = r$.

Casos particulares. — 1. Si A es conmutativo, la hipótesis de ser a permutable con cada uno de los coeficientes de f , se cumple desde luego, y la división generalizada es siempre posible.

2. Si A es íntegro, la hipótesis de no ser a divisor de cero a la izquierda se impone con ello, y la división generalizada, cuando es posible, tiene un resultado único.

Por consiguiente, cuando A es un dominio de integridad, la división generalizada es siempre posible y el resultado es único.

3. Si A tiene un elemento unidad e y si el coeficiente director a de f es igual a e , existe un par, y uno solo de polinomios $q, r \in A[x]$ tales que

$$p(x) = f(x)q(x) + r(x),$$

con

$$r = 0 \quad \text{ó} \quad \text{grado de } r < m$$

puesto que para $a = e$, las dos hipótesis concernientes a a , en el teorema 3, se verifican. Se tiene así la división propiamente dicha (con resto, y a la derecha)

de p por f .

4. Si A es un cuerpo K (que no suponemos conmutativo) pongamos

$$\bar{f}(x) = f(x) \cdot a^{-1}$$

Según el caso precedente, existe un par único $\bar{q}, \bar{r}$ verificando

$$p(x) = \bar{f}(x) \bar{q}(x) + \bar{r}(x)$$

con

$$\bar{r} = 0 \quad \text{o grado de } \bar{r} < m.$$

Se deduce

$$p(x) = f(x) q(x) + r(x)$$

donde

$$q(x) = a^{-1} \bar{q}(x), \quad r(x) = \bar{r}(x),$$

La división propiamente dicha es, pues, siempre posible, y, además con resultado único.

Observación. — Este caso importante se aborda directamente: si

$$f = ax^m + a_1x^{m-1} + \dots$$

$$p = bx^n + b_1x^{n-1} + \dots$$

encontraremos, para los coeficientes sucesivos del cociente

$$q = cx^{n-m} + c_1x^{n-m-1} + \dots$$

las expresiones

$$c = a^{-1}b$$

$$c_1 = a^{-1}b_1 - a^{-1} \cdot a_1 a^{-1} \cdot b$$

$$c_2 = a^{-1}b_2 - a^{-1} a_1 a^{-1} b_1 + a^{-1} (a_1 a^{-1})^2 b - a^{-1} a_2 a^{-1} \cdot b$$

.....

y el método precedente explica la forma.

§ 6. Propiedades aritméticas en los dominios de integridad con elemento unidad. Anillos factoriales. Anillos euclídeos

Sea ahora A un *anillo conmutativo con elemento unidad e* .

Como hemos visto en § 2, las *unidades* de A (es decir, los elementos u que admiten un inverso u^{-1}) forman un grupo multiplicativo U . Estas unidades desempeñan un importante papel en el estudio de las propiedades aritméticas del anillo A , es decir, en las propiedades ligadas a la relación de divisibilidad, definida de la forma siguiente:

Definición. — Dados dos elementos a y b del anillo conmutativo A , diremos que b divide a a , o que b es un divisor de a , o, todavía, que a es un múltiplo de b , si existe en A al menos un elemento q para el cual se tiene:

$$a = bq \quad (q \in A).$$

Se escribe entonces $b \mid a$ ó $a \equiv 0 \pmod{b}$ (a congruente con cero, módulo b);¹ q es el cociente (exacto) de a por b .

Como es $a = ae$, todo elemento a se divide a sí mismo, luego la relación de divisibilidad es *reflexiva*. Es también *transitiva* ($c \mid b$ y $b \mid a$ implica $c \mid a$) ya que de $a = bq$ y $b = cq'$ se deduce $a = cq'q$.

Otras propiedades inmediatas son las siguientes:

1. *Todo divisor del elemento unidad e es una unidad u , e inversamente, toda unidad u divide a e . Todo divisor b de una unidad u es una unidad (pues $u = bq$ implica $bqu^{-1} = e$).*

2. *Todo elemento a del anillo A es múltiplo de cualquier unidad u , y el cociente $q = u^{-1}a$ está unívocamente determinado.*

3. La relación $\mathcal{R}$ definida por

$$x\mathcal{R}x' \quad \text{si} \quad x = x'u, \quad \text{donde } u \text{ es una unidad,}$$

es *reflexiva*, *simétrica* y *transitiva*: es, por esto, una relación de equivalencia en el anillo A . Dos elementos x, x' que la verifican, se llaman *asociados*. Elementos asociados son, pues, los que difieren en factores unidad.

¹ La notación $b \mid a$ hace inútil la expresión equivalente $a = \dot{b}$, que algunos libros utilizan. (N. del T.)

*Todo elemento asociado a un divisor de a es también divisor de a .
Para dos elementos asociados, x, x' tenemos a la vez $x \mid x'$ y $x' \mid x$.*

Definición. — Los elementos asociados de x y las unidades se llaman *divisores impropios* de x ; los otros divisores, si existen, se dicen *propios*; un elemento que no tiene divisores propios y no es una unidad se llama *irreducible*.

Todos los elementos asociados de un elemento irreducible, son también irreducibles.

Observación. — Se ve inmediatamente que la equivalencia $\mathcal{R}$ es regular para la multiplicación. El conjunto cociente $A/\mathcal{R}$ es pues un semigrupo multiplicativo homomorfo al semigrupo multiplicativo A ; $A/\mathcal{R}$ admite a U por elemento neutro, y no tiene más elemento inversible que U . Para cualquier elemento X de $A/\mathcal{R}$, todo divisor distinto de U y X es un divisor propio.

Supongamos ahora que A es un dominio de integridad. Esta hipótesis permite demostrar el siguiente recíproco.

4. En un dominio de integridad si $x \mid x'$ y $x' \mid x$, x y x' son asociados. En efecto, de $x' = xq$ y $x = x'q'$ deducimos:

$$x = xqq' \quad \text{o} \quad x(e - qq') = 0.$$

Si $x = 0$, se tiene $x' = 0$, luego x y x' son asociados. Si x no es nulo, se sigue $qq' = e$, luego q y q' son unidades, con lo que x y x' son, también en este caso, asociados.

Definición. — Se llama *anillo factorial* (o anillo con factorización única, o anillo gaussiano (= de Gauss)) un dominio de integridad con elemento unidad, en el cual:

1) Todo elemento a que no sea unidad, es producto finito de elementos irreducibles (distintos o no)

$$a = p_1 p_2 \dots p_r = \prod_{i=1}^r p_i$$

conviniendo que, para un elemento irreducible, vale una representación de este tipo con $r = 1$.

2) Esta descomposición es única salvo el orden, y salvo factores iguales a unidades.

Esta última condición significa, de manera más explícita, que si un elemento a admite las dos descomposiciones:

$$a = p_1 \dots p_r = q_1 \dots q_s$$

donde las q_i y las p_j son irreducibles, se tiene $s = r$, y, si se ordenan convenientemente las q_j , p_i y q_i son asociados ($i = 1, 2, \dots, r$).

Si A , es un anillo factorial, el semigrupo cociente $A/\mathcal{R}$ es también factorial, como se ve fácilmente, y todo elemento de $A/\mathcal{R}$ es, de una sola forma, salvo el orden, producto finito de elementos irreducibles.

Teorema 1. — Sea A un dominio de integridad con elemento unidad en el cual todo elemento que no sea unidad es producto finito de elementos irreducibles, es decir, cumpliendo la anterior condición 1). Tal anillo es factorial si, y sólo si, satisface a la siguiente condición:

2') todo elemento irreducible p que divide a un producto ab divide al menos a uno de los factores (condición de Gauss).

Supongamos A factorial (condiciones 1) y 2); sea p un elemento irreducible que divide al producto ab :

$$ab = pc$$

Los elementos a y b no son ambos unidades, y si a , por ejemplo, es unidad, es inmediato que p divide a b .

Sean pues:

$$a = \prod_{i=1}^r p'_i, \quad b = \prod_{j=1}^s p''_j, \quad c = \prod_{l=1}^t q_l$$

las descomposiciones de a , b , c , en factores irreducibles. Tenemos:

$$\prod_{i=1}^r p'_i \cdot \prod_{j=1}^s p''_j = p \cdot \prod_{k=1}^t q_k$$

Según la condición 2), p es asociado de uno de los elementos p'_i , p''_j , por lo que p divide al menos a uno de los elementos a , b .

Demostremos ahora que 2') implica 2). Razonaremos por recurrencia sobre

el número r de factores irreducibles que figuran en la primera descomposición de a . La proposición es evidentemente cierta para $r = 1$, por la definición de elemento irreducible. Supongamos ahora el teorema cierto cuando la primera descomposición tiene menos de r factores ($r > 1$) y sea

$$a = \prod_{i=1}^r p_i = \prod_{j=1}^s q_j.$$

El elemento irreducible p_1 divide a

$$q_1 \cdot \prod_{j=2}^s q_j,$$

por consiguiente, o divide a q_1 , o divide a

$$\prod_{j=2}^s q_j;$$

se ve así, reiterando, que uno al menos de los q_j es divisible por p_1 . Supongamos la numeración de subíndices tomada de forma que este sea q_1 : puesto que q_1 es irreducible y p_1 no es unidad, p_1 y q_1 son asociados: $q_1 = \epsilon_1 p_1$, donde ϵ_1 es una unidad:

En el dominio de integridad A , el elemento $p_1 \neq 0$ es simplificable; se obtiene por tanto la igualdad:

$$p_2 \dots p_r = \epsilon_1 q_2 \dots q_s = q'_2 \dots q_s$$

(donde $q'_2 = \epsilon_1 q_2$ es irreducible); y, según la hipótesis de recurrencia, el teorema está demostrado.

Estudiemos las *propiedades aritméticas* de los elementos del anillo factorial A que no son unidades. Sea:

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \quad (p_i \neq p_j, \alpha_i \geq 1)$$

uno de tales elementos, descompuesto en factores irreducibles (aquí es cómodo, no escribir más que los factores *distintos*, afectando a cada uno de su exponente). Si otro elemento a' divide a a , cada uno de sus factores irreducibles, también divide a a , luego es asociado de algún p_i , y el exponente α'_i con el que figura en a' , no es mayor que α_i . Por tanto, *todos los divisores de a , resultan, salvo factores unidad, como los productos formados con los factores irreduci-*

bles p_i de a afectados de exponentes α_i limitados así: $0 \leq \alpha_i \leq a_i$.

La formación de los divisores comunes a dos elementos $a, b (\notin U)$ se deduce inmediatamente.

Es cómodo ahora escribir la descomposición factorial en la forma

$$a \equiv p_1^{\alpha_1} \dots p_\rho^{\alpha_\rho} \quad (\mathcal{R}), \quad b \equiv p_1^{\beta_1} \dots p_\rho^{\beta_\rho} \quad (\mathcal{R}), \quad (\alpha_i, \beta_i \geq 0),$$

siendo los p_i los factores irreducibles distintos que figuran en *uno al menos* de los elementos a, b . Para todo divisor común h , tenemos:

$$h \equiv p_1^{\lambda_1} \dots p_\rho^{\lambda_\rho} \quad (\mathcal{R}), \quad \text{con} \quad 0 \leq \lambda_i \leq \delta_i,$$

donde hemos puesto

$$\delta_i = \min (\alpha_i, \beta_i).$$

Todos estos divisores comunes dividen a uno de ellos:

$$d = p_1^{\delta_1} \dots p_\rho^{\delta_\rho}$$

al que se llama, por esta razón, *máximo común divisor* de a y b , y se escribe m.c.d. (a, b) . Como es claro la unicidad de esta expresión no es estricta, sino a menos de factores que sean unidades de A .

Igualmente, para todo múltiplo común k , tenemos:

$$k \equiv p_1^{\kappa_1} \dots p_\rho^{\kappa_\rho} (\mathcal{R}), \quad \text{con} \quad \mu_i \leq \kappa_i$$

donde hemos puesto

$$\mu_i = \max (\alpha_i, \beta_i).$$

Todos estos múltiplos comunes de a y b son los múltiplos de uno de ellos:

$$m = p_1^{\mu_1} \dots p_\rho^{\mu_\rho}$$

llamado mínimo común múltiplo de a y b y lo designaremos por m.c.m. (a, b) . Tal elemento queda determinado sólo a menos, como antes, de factores que sean unidades de A .

Se tiene evidentemente

$$\min (\alpha, \beta) + \max (\alpha, \beta) = \alpha + \beta$$

y por consiguiente

$$dm = ab.$$

Se definen de modo análogo el máximo común divisor y el mínimo común múltiplo de un conjunto de k elementos $a_1, a_2, a_3, \dots, a_k$ de A . Ambos elementos, como para $k = 2$, sólo están determinados a menos de factores unidades; se pueden calcular a partir de la descomposición de las a_i en factores irreducibles, y las reglas para ello son una generalización inmediata de las precedentes.

En un *dominio de integridad* D , con elemento unidad e , la noción aritmética clásica de números primos entre sí, admite tres generalizaciones posibles, que son las siguientes:

I. Diremos que dos elementos a, b de $D^* = D - \{0\}$ no tienen divisores comunes, si todo elemento de D^* que divide a a y a b , es una unidad. En el caso particular de un anillo factorial, esta propiedad equivale a

$$\text{m. c. d. } (a, b) = 1$$

II. Cada uno de los elementos a, b , es primo con el otro; con esto entendemos, por definición, que a es primo con b , cuando para todo x de D , el hecho de que b divida a ax , exige que b divida a x . Demostremos que entonces también es b primo con a . Supongamos que a divide a by , es decir, $by = ax$; entonces por la hipótesis, b divide a x , $x = bq$, de donde $y = aq$, luego a divide a y .

Esta propiedad II, o sea, el hecho de ser a primo con b implica la propiedad I, pues, si h es un divisor común se tiene

$$a = a'h, \quad b = b'h$$

de donde

$$ab' = ba'$$

y por consiguiente b divide a b' ; b y b' son, pues, asociados, h es una unidad.

En un anillo factorial, el recíproco es cierto: I implica II. En efecto, si a y b no tienen divisores comunes, no tendrán, en particular, ningún factor irreducible común y, si b divide a ax , todo factor irreducible p que figure en b con exponente $\beta (> 0)$ debe figurar en x con un exponente al menos igual a β ; resulta de esto que b divide a x .

III. Diremos que dos elementos a, b del dominio de integridad D verifican una relación de Bezout si existen dos elementos x, y de D tales que sea:

$$xa + yb = e$$

Entonces, todo divisor común a a y a b divide a e , es decir, es una unidad: III implica I. Incluso en los anillos factoriales, el recíproco no es cierto en general, como veremos más adelante.

Indiquemos algunos tipos importantes de anillos factoriales.

1.º *Todo cuerpo conmutativo K es un anillo factorial; en este caso no hay elementos irreducibles, ya que todos los elementos no nulos de K son unidades.*

2.º *En el anillo de los enteros $\mathbf{Z}$, los elementos irreducibles se llaman números primos (la costumbre de no considerar el 1 como número primo responde al hecho de que un elemento irreducible no es una unidad).*

Sea m un número cualquiera. Si m no es primo, admite un divisor propio m_1 y se tiene la descomposición $m = m_1 m_2$, donde m_1 y m_2 son menores que m en valor absoluto. Si m_1 y m_2 no son los dos primos el razonamiento se repite, y se llega necesariamente, al cabo de un número finito de operaciones, a una descomposición

$$m = p_1 \dots p_r \quad (r \geq 1)$$

donde los p_i son primos; $\mathbf{Z}$ verifica pues la condición 1).

Para demostrar que el anillo de los enteros es un anillo factorial, estableceremos la condición 2'), dando una demostración directa, sin utilizar la teoría del m.c.d.

Teorema 2 (teorema de Gauss). — *En el anillo de los enteros $\mathbf{Z}$, si un número primo p divide al producto ab y no divide a b , es p divisor de a .*

Puesto que p no divide a b , p es distinto de b . Si p es inferior a b , efectuemos la división (con resto)

$$b = pq + r, \quad 0 \leq r < p.$$

Multiplicando los dos miembros por a , vemos que p divide al producto ar mientras que no divide a r . Hemos reducido así la cuestión al caso en que p es superior a b . El producto ab pertenece al conjunto $a, 2a, \dots, (p-1)a$. Sea m el menor entero natural, tal que p divida a ma ; tenemos $1 \leq m \leq b \leq p-1$ y si $m = 1$ el teorema está demostrado. Si m es mayor que 1, tendremos, dividiendo p por m :

$$p = q'm + r', \quad 0 \leq r' < m$$

siendo en realidad $0 < r'$ puesto que p es primo; resultaría de aquí, multiplicando por a , que p divide a ar' , lo cual es contradictorio.

Dominio o anillo euclídeo $\mathfrak{E}$.

Definición. — Se llama *anillo euclídeo* $\mathfrak{E}$ un dominio de integridad en el cual se ha definido una aplicación en el conjunto de los enteros ≥ 0 asociando a todo elemento a no nulo de $\mathfrak{E}$ el entero $\varphi(a)$ con las condiciones:

I. Si b divide a a : $\varphi(b) \leq \varphi(a)$.

II. Si a y b son dos elementos cualesquiera de $\mathfrak{E}$, $b \neq 0$, existen q y r , elementos de $\mathfrak{E}$, tales que $a = bq + r$ con, si $r \neq 0$, $\varphi(r) < \varphi(b)$.

(si $r = 0$, b divide a a , se tiene la condición I.)

Un anillo euclídeo es pues, un anillo en el cual existe una división con resto.

Ejemplos de anillos euclídeos.

1.º El anillo $K[x]$ de los polinomios en x sobre un cuerpo conmutativo K es un dominio de integridad; a todo elemento $f(x)$ asociamos $\varphi(f) = \text{grado de } f$, número positivo o nulo que cumple las condiciones I y II. $K[x]$ es, pues, un anillo euclídeo.

2.º En el anillo de los enteros, definiremos $\varphi(n) = |n|$, con lo que vemos inmediatamente que es un anillo euclídeo.

En tales anillos, tenemos las propiedades siguientes:

1. *Un anillo euclídeo posee elemento unidad.* Sea a uno de los elementos del anillo para los cuales $\varphi(a)$ tiene el valor mínimo. La condición II, aplicada al par (a, a) nos asegura la existencia de q y r tales que:

$$a = qa + r.$$

Pero $\varphi(r) < \varphi(a)$ es imposible, por la elección de a ; se tiene, pues $r = 0$ y existirá una q tal, que:

$$a = qa.$$

Sea entonces x un elemento cualquiera del anillo:

$$xa = xqa$$

implica $(x - qx)a = 0$. Ahora bien, estamos en un dominio de integridad y a

es diferente de cero (puesto que $\varphi(a)$ está definido). Se tiene, pues, $x - qx = 0$ y q es elemento unidad del anillo. Lo designaremos por 1; $a = 1a$ para todo a implica $\varphi(1) \leq \varphi(a)$ para todo a de $\mathfrak{E} - \{0\}$.

2. La propiedad $\varphi(\xi) = \varphi(1)$ caracteriza a las unidades ξ . Primeramente si ξ es una unidad, ξ divide a 1 y la condición I da $\varphi(\xi) \leq \varphi(1)$, de donde, puesto que $\varphi(1) \leq \varphi(a)$ para todo a :

$$\varphi(\xi) = \varphi(1)$$

Recíprocamente, $\varphi(\xi) = \varphi(1)$ implica que ξ es una unidad, es decir, que ξ es asociado de 1. En efecto, como 1 divide a todo elemento, lo enunciado resulta de la propiedad siguiente:

3. En un anillo euclídeo, si b divide a a ($a = bq'$) y $\varphi(a) = \varphi(b)$, a y b son asociados.

Se tiene, por II, $b = aq + r$. Si $r = 0$, esta relación se transforma en $b = aq$ que junto con $a = bq'$ nos dice que a y b son asociados. Si r no es nulo, se tiene (por II) $\varphi(r) < \varphi(a) = \varphi(b)$ mientras que la relación $r = b - aq = b(1 - qq')$ lleva consigo $\varphi(b) \leq \varphi(r)$; r es, pues, necesariamente nulo y a y b son asociados.

Teorema 3. — En un anillo euclídeo $\mathfrak{E}$, dos elementos a y b de $\mathfrak{E} - \{0\}$ sin divisores comunes, verifican una identidad de Bezout.

Consideremos el conjunto $\mathfrak{J}$ de los elementos de $\mathfrak{E} - \{0\}$ de la forma:

$$\alpha a + \beta b \quad \text{donde} \quad \alpha \in \mathfrak{E}, \quad \beta \in \mathfrak{E}$$

y el conjunto de los enteros $\varphi(\alpha a + \beta b)$. Sea d uno de los elementos de $\mathfrak{J}$ para los cuales este entero es mínimo:

$$d = \alpha^* a + \beta^* b.$$

La condición II nos asegura la existencia en $\mathfrak{E}$ de elementos s y t tales, que

$$a = ds + t, \quad \text{con} \quad t = 0 \quad \text{ó} \quad t \neq 0 \text{ y } \varphi(t) < \varphi(d).$$

Pero como, si t no es nulo, es $t = a - ds = a(1 - s\alpha^*) - s\beta^* b$, este elemento pertenece a $\mathfrak{J}$, y no puede ser que $\varphi(t) < \varphi(d)$. Luego es $t = 0$, y d divide a a y, lo mismo, d divide a b . Luego, todo divisor de d , es un divisor común a a y a b . Pero como, por otra parte, $d = \alpha^* a + \beta^* b$ hace ver que todo divisor común de a y b es un divisor de d , resulta que d es el máximo común divisor de a y b , y lo mismo todos sus asociados. Con esto hemos demostrado: en un anillo euclí-

de dos elementos cualesquiera a y b de $\mathfrak{E} - \{0\}$ admiten un máximo común divisor que se pone bajo la forma

$$d = \alpha a + \beta b \quad (\alpha \in \mathfrak{E} - \{0\}, \beta \in \mathfrak{E} - \{0\}).$$

En particular, cuando a y b no tienen otro divisor común que las unidades, están ligados por una relación de la forma

$$1 = \alpha a + \beta b$$

Por lo tanto: *En un anillo euclídeo, los conceptos I y III de elementos primos entre sí, son idénticos.*

Teorema 4. — *Un anillo euclídeo es un anillo factorial.*

Vamos a demostrar:

1. Todo elemento a de $\mathfrak{E} - \{0\}$ distinto de las unidades, es un producto finito de factores irreducibles.

2'. Si p es irreducible y divide a un producto ab , divide a uno de los factores.

Haremos la demostración por recurrencia sobre los valores de $\varphi(a)$.

Si $\varphi(a) = \varphi(1)$, se ha visto que esto implica que a sea una unidad; la propiedad es, pues, verdadera para $\varphi(a) = \varphi(1)$. Supondremos el teorema cierto para todo a' con $\varphi(a') < \varphi(a)$ y lo demostraremos para el elemento a .

Si a es irreducible la propiedad está demostrada.

Si a no es irreducible se tiene $a = bc$, donde ni b ni c son asociados a a , y $\varphi(b) < \varphi(a)$; $\varphi(c) < \varphi(a)$, puesto que, si en un anillo euclídeo b divide a a y $\varphi(a) = \varphi(b)$, resulta que a y b son asociados; entonces, en virtud de la hipótesis de inducción, b y c son ambos producto finito de elementos irreducibles: ocurre, pues, lo mismo para a .

Demostremos ahora la propiedad 2'. Sea p irreducible, $p \in \mathfrak{E}$. Supongamos que p divide a ab y no divide a a ; entonces p y a no tienen divisores comunes y existen $\alpha \in \mathfrak{E}$ y $\beta \in \mathfrak{E}$ tales que

$$1 = \alpha a + \beta p,$$

de donde

$$b = \alpha ab + \beta bp,$$

que demuestra, puesto que p divide a ab , que p divide a b .

Sea A un anillo factorial. Nos proponemos establecer el teorema de *transfencia* siguiente:

Teorema 5. — Si A es un anillo factorial, el anillo de los polinomios $P_1 = A[x]$ es también un anillo factorial.

De este teorema resulta, de paso en paso, que el anillo de los polinomios $P_r = A[x_1, \dots, x_r]$ es también un anillo factorial.

Sabemos que P_1 es un dominio de integridad (§ 5, teorema 2) y tiene como elemento unidad el mismo e de A .

Para establecer en P_1 las propiedades 1) y 2') que, según el teorema 1, llevan consigo que P_1 sea factorial, tenemos necesidad de algunos preliminares.

Dado un polinomio $f(x) \in A[x]$, designemos por c y llamemos *factor constante*¹ al m.c.d. de los coeficientes de f ; escribamos

$$f(x) = cf^*(x)$$

donde $f^*(x) \in A[x]$ tiene sus coeficientes sin más divisores comunes que las unidades. Un polinomio así, en el que los coeficientes no tienen divisores comunes se llama *primitivo*.

Cualquier polinomio de $A[x]$ es pues producto de un polinomio primitivo por una constante, y esta descomposición es única salvo factores iguales a las unidades de A (o, lo que es lo mismo, de $A[x]$). Un polinomio irreducible de $A[x]$ de grado $n > 0$, es necesariamente primitivo; una constante es elemento irreducible de $A[x]$ si, y sólo si, es irreducible en A .

Cualquier constante es así, en $A[x]$, el producto de un número finito de elementos irreducibles, siendo esta descomposición la que, por hipótesis, existe en A . Para establecer la existencia de una descomposición en factores irreducibles en $A[x]$ podemos pues razonar por recurrencia sobre el grado n del polinomio f considerado.

Podemos suponer que f es *primitivo*. Si f no es irreducible, admitirá una descomposición $f = f_1 f_2$, en la que cada divisor propio f_1, f_2 de f es un polinomio de grado no nulo. Estos polinomios son de grado estrictamente inferior a n y según la hipótesis de recurrencia pueden descomponerse en productos finitos de factores irreducibles. Lo mismo ocurrirá con f , lo que demuestra que la condición 1) del teorema 1 se cumple en $A[x]$.

Para establecer la condición 2') utilizaremos las siguientes proposiciones.

Lema 1. — Si un elemento irreducible p de A divide a los coeficientes $a_0, \dots, a_{r-1}, b_0, \dots, b_{s-1}$, pero no divide ni a a_r ni a b_s , este p no dividirá al coeficiente c_{r+s} de x^{r+s} en el producto de los dos polinomios f y g siguientes:

$$\begin{aligned} f(x) &= a_0 + a_1x + \dots + a_rx^r + \dots \\ g(x) &= b_0 + b_1x + \dots + b_sx^s + \dots \end{aligned}$$

¹ En otros textos se le llama *factor contingente*. (N. del T.)

Tendremos en efecto

$$c_{r+s} = (\dots + a_{r-1}b_{s+1}) + a_r b_s + (a_{r+1}b_{s-1} + \dots)$$

y p divide a cada uno de los paréntesis, pero no al producto $a_r b_s$, por ser irreducible.

Lema 2. — *El producto $f^* g^*$ de dos polinomios primitivos es primitivo.*

Bastará demostrar que dado un elemento irreducible cualquiera p de A , p no divide a todos los coeficientes del producto $f^* g^*$. Ahora bien, p no divide a todos los coeficientes de ninguno de los dos polinomios primitivos f^*, g^* , por lo que el lema 2 resulta consecuencia del teorema 1.

Dicho esto considerando dos polinomios descompuestos en factor constante y polinomio primitivo

$$f_i(x) = c_i f_i^*(x) \quad (i = 1, 2)$$

para el producto $f(x)$ tendremos

$$f(x) = c_1 c_2 f_1^*(x) f_2^*(x)$$

y como el producto $f_1^* f_2^*$ es primitivo, la igualdad precedente nos da la descomposición de f en factor constante y polinomio primitivo.

Lema 3. — *Si un polinomio primitivo $g^*(x)$ divide en $A[x]$ un producto $kf(x)$, siendo k una constante, g^* divide a f .*

Tendremos

$$kf(x) = g^*(x)q(x) = mg^*(x)q^*(x)$$

donde m es el factor constante y q^* el polinomio primitivo del cociente $q(x)$. El producto $g^*(x)q^*(x)$ es primitivo, luego la constante k , por dividir a todos los coeficientes del polinomio mg^*q^* , dividirá a m , $m = m'k$, de donde.

$$f(x) = g^*(x) m' q^*(x)$$

como queríamos demostrar.

Demostremos ahora que la condición (2') se cumple en $A[x]$, es decir, que si un polinomio irreducible $p(x)$ divide al producto $f(x)g(x)$, divide por lo menos a uno de los dos polinomios f, g .

Si $p(x)$ es una constante, $p(x) = p \in A$; p divide a $f(x)g(x)$ es decir, poniendo de manifiesto los polinomios primitivos, $cdf^*(x)g^*(x)$. Ahora, según el lema 2, el producto f^*g^* es primitivo; en consecuencia p divide a cd y, por ser p elemento irreducible de A , p divide a uno al menos de los factores c, d y en consecuencia a uno al menos de los polinomios f, g .

Supongamos ahora $p(x)$ de grado positivo y demostremos que, si p no divide a f debe dividir a g .

En el conjunto M de polinomios de la forma

$$u(x)p(x) + v(x)f(x)$$

donde $u(x), v(x)$ son polinomios del anillo $A[x]$, consideremos uno de los polinomios de grado mínimo, sea $m(x)$; sean μ su grado y a su coeficiente director. Existen un entero $k \geq 0$ y polinomios $q(x), r(x)$ tales que se tenga

$$a^k f(x) = m(x)q(x) + r(x)$$

con

$$r = 0 \quad \text{o} \quad \text{grado } r < \mu.$$

Por hipótesis, $m(x)$ es de la forma

$$(1) \quad m(x) = u(x)p(x) + v(x)f(x)$$

y tendremos

$$r(x) = -u(x)q(x)p(x) + [a^k - v(x)q(x)]f(x) \in M$$

lo que implica $r = 0$, de donde

$$a^k f(x) = m(x)q(x).$$

Poniendo de manifiesto en $m(x)$ el polinomio primitivo m^* tendremos

$$(2) \quad m(x) = m_0 m^*(x), \quad m_0 \in A$$

m^* dividirá a $a^k f(x)$ y por lo tanto a $f(x)$ según el lema 3.

Efectuando del mismo modo la división generalizada de $p(x)$ por $m(x)$, se ve que m^* divide a p . Ahora bien, p es irreducible. Si m^* estuviese asociado a p , en $A[x]$, p dividiría a f contrariamente a la hipótesis; en consecuencia, m^* es unidad de $A[x]$, y por lo tanto de A . Tendremos entonces según (1) y (2)

$$m_0 g(x) = m^{*-1} (u g p + v f g)$$

y p , por dividir a fg , dividirá a $m_0g(x)$. Pero entonces $p(x)$, polinomio irreducible y por lo tanto primitivo dividirá a $g(x)$, según el lema 3, lo que establece el teorema.

Consideremos en fin, para dar un ejemplo de anillo que no es factorial, el anillo A de los números complejos de la forma $a + b\sqrt{-5}$, donde a y b son enteros de cualquier signo. El elemento unidad de A es el número 1, y como subanillo del cuerpo de los complejos A es un dominio de integridad.

Para que $x + y\sqrt{-5}$ ($x, y \in \mathbf{Z}$) divida a $a + b\sqrt{-5}$, es decir, para que

$$a + b\sqrt{-5} = (x + y\sqrt{-5})(x' + y'\sqrt{-5})$$

es necesario y suficiente que

$$\begin{cases} a = xx' - 5yy' \\ b = xy' + yx' \end{cases}$$

de donde

$$a - b\sqrt{-5} = (x - y\sqrt{-5})(x' - y'\sqrt{-5})$$

y

$$a^2 + 5b^2 = (x^2 + 5y^2)(x'^2 + 5y'^2)$$

Luego, para que $x + y\sqrt{-5}$ divida a $a + b\sqrt{-5}$, es necesario que $x^2 + 5y^2$ divida a $a^2 + 5b^2$, lo que permite encontrar los divisores de $a + b\sqrt{-5}$; se ve así que su número es finito.

En particular se constata (tomando $a = 1$, $b = 0$) que las únicas unidades de A son $+1$ y -1 .

También se ve fácilmente que 3 , $2 + \sqrt{-5}$, $2 - \sqrt{-5}$ son elementos irreducibles de A .

El elemento irreducible $2 + \sqrt{-5}$ es divisor de

$$3^2 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

sin dividir a 3 , y el 9 admite dos descomposiciones distintas en factores irreducibles. El anillo A no es pues un anillo factorial. Este ejemplo debido a Dedekind, ha tenido un papel importante en la fundación de la teoría de los ideales creada para suplir la factorización de elementos de los anillos no factoriales.

§ 7. Ideales de un anillo

En un anillo A , que no suponemos conmutativo, sea $\mathcal{R}$ una relación de equivalencia compatible con la adición y con la multiplicación del anillo. Asociando a cada elemento x de A la clase X módulo $\mathcal{R}$ a la que pertenece definiremos una aplicación exhaustiva φ de A sobre el conjunto cociente $A/\mathcal{R}$ y, como ya sabemos, podremos definir en $A/\mathcal{R}$ una adición y una multiplicación¹ que hacen de φ un homomorfismo y de $A/\mathcal{R}$ la imagen homomorfa de A , $\varphi(A)$.

De un modo general, sea h un homomorfismo de un anillo A en un conjunto A' con una adición y una multiplicación, es decir, una aplicación de A en A' compatible de una parte con las adiciones de A y de A'

$$h(x + y) = h(x) + h(y) \quad \forall x, y \in A$$

y de otra parte con las multiplicaciones de A y de A'

$$h(xy) = h(x) \cdot h(y) \quad \forall x, y \in A.$$

Se tiene la siguiente proposición:

Teorema 1. — *La imagen $\overline{A} = h(A)$ de un anillo A en un homomorfismo h es un anillo. En particular el cociente $A/\mathcal{R}$ del anillo A por una equivalencia compatible con la adición y la multiplicación de A es un anillo, que se llama anillo cociente de A por $\mathcal{R}$.*

La demostración de este teorema deriva inmediatamente de las proposiciones anteriores. Respecto a la adición, $\overline{A}$ es un grupo abeliano; por otra parte, $\overline{A}$ es un semigrupo multiplicativo y su multiplicación es distributiva respecto a su adición; luego $\overline{A}$ es un anillo.

Desde el punto de vista aditivo, el núcleo $\mathfrak{m}$ del homomorfismo h definido como imagen inversa del cero $\overline{0}$ de $\overline{A}$:

$$\mathfrak{m} = h^{-1}(\overline{0}) = \{ m ; m \in A, h(m) = \overline{0} \},$$

es un subgrupo del grupo abeliano aditivo A .

Desde el punto de vista multiplicativo, $\mathfrak{m}$, imagen inversa del elemento lícito $\overline{0}$ es una parte lícita de A [cap. I, § 8, teor. 5. Por lo demás, inmediatamente resulta, $\forall m \in \mathfrak{m}$ y $\forall x \in A$, $h(mx) = h(m)h(x) = \overline{0}h(x) = \overline{0}$, luego $mx \in \mathfrak{m}$ y $xm \in \mathfrak{m}$].

¹ Si X e Y son dos clases que contienen respectivamente a los elementos x e y , $X + Y$ es la clase que contiene a $x + y$, e XY es la clase que contiene a xy (capítulo I, § 4, 6.º).

Estas dos propiedades del núcleo conducen a la siguiente definición:

Definición. — Se llama *ideal bilátero* de un anillo A a cualquier subgrupo aditivo de A que sea, además, *lícito multiplicativamente*. Es decir, a todo subconjunto no vacío $\mathfrak{m}$ que verifica las dos condiciones

- 1) $m_1 \in \mathfrak{m}$ y $m_2 \in \mathfrak{m}$ implican $m_1 - m_2 \in \mathfrak{m}$;
- 2) $m \in \mathfrak{m}$ implica, $\forall x \in A$, $xm \in \mathfrak{m}$ y $mx \in \mathfrak{m}$.

Teorema 2 (teorema de homomorfismo para los anillos). — Sea h un homomorfismo que aplica un anillo A sobre un anillo $\bar{A} = h(A)$.

- 1.º el núcleo $\mathfrak{m} = h^{-1}(\bar{0})$ de este homomorfismo es un ideal bilátero;
- 2.º la equivalencia de homomorfismo $\mathcal{R}$ se define a partir de $\mathfrak{m}$ por

$$a_1 \equiv a_2 \quad (\mathcal{R}) \quad \text{si} \quad a_1 - a_2 \in \mathfrak{m}.$$

- 3.º Se tiene el isomorfismo

$$\bar{A} \simeq A/\mathfrak{m}$$

donde $A/\mathfrak{m}$ designa el anillo cociente $A/\mathcal{R}$ de A por $\mathcal{R}$.

La primera parte del teorema acaba de ser establecida, bastando tener en cuenta, además, la definición de ideal bilátero.

La segunda parte resulta del hecho de que h es, en particular, un homomorfismo que aplica el grupo aditivo A sobre el grupo aditivo $\bar{A}$, siendo su núcleo el subgrupo aditivo $\mathfrak{m}$.

Por la misma razón, la aplicación biyectiva que asocia a cada elemento $\bar{x}$ de $\bar{A}$ la clase $X (\in A/\mathfrak{m})$, conjunto de elementos x de A que tienen $\bar{x}$ por imagen $h(x) = \bar{x}$, es un isomorfismo de grupos aditivos. Por otra parte, es claro que esta aplicación respeta la multiplicación, luego es, efectivamente, un isomorfismo de anillos, lo que demuestra la tercera parte.

Teorema 3. — Recíprocamente, para cualquier ideal bilátero $\mathfrak{m}$ de un anillo A la relación $\mathcal{R}$ que se define en A por

$$a\mathcal{R}b \quad \text{si} \quad a - b \in \mathfrak{m}$$

es: 1.º una relación de equivalencia compatible con la adición de A ; 2.º una relación compatible con la multiplicación de A . En consecuencia el conjunto cociente $A/\mathcal{R}$, designado más cómodamente por $A/\mathfrak{m}$, es un anillo imagen homomorfa de A .

Puesto que $\mathfrak{m}$ es un subgrupo aditivo de A , la relación $\mathcal{R}$, es una equiva-

lencia compatible con la adición, según los teoremas establecidos para los grupos. Además es regular a la derecha para la multiplicación puesto que $a \equiv b(\mathcal{R})$, o bien $a - b = m \in \mathfrak{m}$ implica $(a - b)x = mx \in \mathfrak{m}$, es decir $ax \equiv bx(\mathcal{R})$. Se ve del mismo modo que es regular a la izquierda, y por lo tanto compatible con la multiplicación.

Para módulo $\mathcal{R}$, $\mathfrak{m}$ no es más que la clase que contiene a cero.

Esto dicho, $A/\mathcal{R}$ es imagen homomorfa de A en el homomorfismo canónico luego será, según el teorema 1, un anillo que es usual designar por $A/\mathfrak{m}$ al que se llama *anillo cociente de A por el ideal bilátero $\mathfrak{m}$* . Frecuentemente se escribe $a \equiv b(\mathfrak{m})$ en vez de $a \equiv b(\mathcal{R})$, en el sentido pues, de $a - b \in \mathfrak{m}$.

Según los teoremas precedentes, dado un anillo A , hay correspondencias biyectivas entre las equivalencias $\mathcal{R}$ definidas en A y compatibles con su adición y con su multiplicación, los anillos $\overline{A}$ imágenes homomorfas de A y los ideales biláteros $\mathfrak{m}$ de A .

Consideremos ahora en el anillo A relaciones de equivalencia compatibles con la adición pero a las que supondremos regulares por un solo lado respecto a la multiplicación. Sea, por ejemplo, $\mathfrak{D}$ una equivalencia tal, regular a la derecha para la multiplicación. La clase $\mathfrak{d}$ conjunto de los elementos de A equivalentes a cero módulo $\mathfrak{D}$ es un subgrupo aditivo y un subconjunto multiplicativamente lícito a la derecha: cualquier subconjunto del anillo que tenga ambas propiedades se llamará *ideal a la derecha de A* .

Recíprocamente, demos *a priori* un ideal a la derecha $\mathfrak{d}$ de A . Puesto que es un subgrupo aditivo de A , la relación $\mathfrak{D}$ definida por

$$a \mathfrak{D} b \quad \text{si} \quad a - b \in \mathfrak{d}$$

es compatible con la adición; se ve además (como en la demostración del teorema 3), que es regular a la derecha para la multiplicación.

Para módulo $\mathfrak{D}$, $\mathfrak{d}$ es la clase que contiene al cero.

Teorema 4. — *Dados un anillo A , existen correspondencias biyectivas entre los ideales a la derecha de A y las relaciones de equivalencia definidas en A , compatibles con la adición y regulares a la derecha con respecto a la multiplicación.*

Los ideales a la izquierda se definen en forma simétrica, y para ellos vale un teorema simétrico del anterior.

En cualquier anillo, el subconjunto constituido por el elemento cero únicamente, es un ideal bilátero, llamado *ideal cero* y designado por (0) . También el anillo entero A es un ideal bilátero. Si A posee un elemento unidad e , el ideal A se llama *ideal unidad* y se designa por (e) . Estos dos son los ideales impro-

prios de A y cualquier otro es un ideal *propio*.

Si el anillo A tiene elemento unidad e , y si un elemento a de A es inversible a la derecha, cualquier ideal a la derecha $\mathfrak{d}$ que contenga a a coincide con el ideal unidad, puesto que, si x es un elemento cualquiera de A , se tiene $x = a \cdot a^{-1}x \in \mathfrak{d}$. Resulta de aquí que *un cuerpo K no contiene ideales propios y por lo tanto no admite más imágenes homomorfas que los cuerpos isomorfos*.

Puesto que una parte lícita (incluso a un solo lado) con respecto a una ley de composición es estable para esta ley, *todo ideal de un anillo A es un subanillo*. Las dos nociones no deben confundirse: en el cuerpo de los racionales $\mathbb{Q}$ el anillo de los enteros $\mathbb{Z}$ es un subanillo propio y, según lo que precede, no es un ideal. Los ideales, que pueden ser caracterizados como clases que contienen al 0 relativas a equivalencias notables, o como núcleos de homomorfismos (si se trata de ideales biláteros), desempeñan en la teoría de los anillos un papel mucho más importante que los subanillos; este papel es muy comparable al de los subgrupos distinguidos en la teoría de grupos.

Si el anillo A es conmutativo, las nociones de ideal bilátero, ideal a la izquierda e ideal a la derecha se confunden, y se dice simplemente ideal.

Ejemplos. — 1. En el anillo $\mathbb{Z}$ de los enteros, el conjunto

$$\mathbb{Z}m = \{ km ; k \in \mathbb{Z} \}$$

de los múltiplos de un entero fijo m es un ideal $\mathfrak{m}$; la equivalencia $\mathcal{R}$ correspondiente es la congruencia aritmética módulo m ; el anillo homomorfo asociado es el anillo $\mathbb{Z}/(m)$ de los enteros módulo m .

De este modo se obtienen todos los ideales de $\mathbb{Z}$, pues por ser $\mathbb{Z}$ un grupo monógeno aditivo, todo subgrupo de $\mathbb{Z}$ lo es también. El anillo $\mathbb{Z}$ tiene la propiedad de que todo subgrupo aditivo es un ideal; las equivalencias compatibles con la adición son las congruencias aritméticas, y éstas tienen la propiedad de ser compatibles con la multiplicación.

2. Sea a un elemento de un anillo A . El conjunto $\mathfrak{d}$ de los elementos d del anillo para los que se cumple la igualdad $ad = 0$, es un ideal a la derecha que se llama *anulador a la derecha* de a ; $\mathfrak{d} = (0)$ es la condición necesaria y suficiente para que a no sea divisor de cero a la izquierda.

3. Dados un conjunto cualquiera X y un anillo $A \neq (0)$, consideremos el anillo $\mathcal{F}$ de funciones definidas sobre X que toman sus valores en A (ver § 2, ejemplo 2). Consideremos una parte $S (\neq \emptyset)$ no vacía de X : El conjunto $\mathfrak{n}$ de las funciones $f \in \mathcal{F}$ tales que

$$f(s) = 0 \quad (\in A) \quad \forall s \in S$$

es un ideal bilátero del anillo $\mathcal{F}$.

Para $X = \mathbf{N}$, conjunto de enteros naturales, las funciones se convierten en sucesiones $\{a_i\}$ de elementos de A . Si designamos por $\mathfrak{m}_k$ el conjunto de sucesiones $\{a_i\}$ para las que

$$a_n = 0 \quad \forall n \geq k,$$

habremos definido en el anillo $\mathcal{S}$ de sucesiones consideradas (en el que la adición y la multiplicación se hace término a término) una familia infinita numerable de ideales $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_k, \dots$ en los que se tiene las inclusiones estrictas

$$\mathfrak{m}_1 \subset \mathfrak{m}_2 \subset \dots \subset \mathfrak{m}_k \subset \mathfrak{m}_{k+1} \subset \dots$$

4. Sea A un anillo conmutativo y consideremos el anillo de polinomios $P_r = A[x_1, \dots, x_r]$. Sea S un conjunto de puntos $(a_1, \dots, a_r)$ en el espacio $E = A^r$. El conjunto $\mathfrak{m}$ de los polinomios f de P_r que cumplen la condición

$$f(a_1, \dots, a_r) = 0 \quad \forall (a_1, \dots, a_r) \in S,$$

la que se expresa diciendo que tales polinomios *se anulan sobre el conjunto S* , es un ideal en el anillo P_r .

Para $r = 3$, si A es el cuerpo de los números reales $\mathbf{R}$ o el cuerpo de los complejos Ω , E es lo que se llama espacio euclídeo o espacio cartesiano de tres dimensiones. El conjunto de polinomios $\mathbf{R}[x, y, z]$ o de $\Omega[x, y, z]$ que son nulos en un punto dado, o en k puntos dados, o sobre un conjunto dado de curvas o de puntos es, en cada caso, un ideal.

La ley que a cada polinomio f de P_r asocia su término constante $c = f(0, \dots, 0) \in A$ es un homomorfismo que aplica al anillo P_r sobre el anillo A . El núcleo de este homomorfismo es el ideal de polinomios nulos en el punto $(0, \dots, 0)$.

Si A es un anillo que no supondremos conmutativo, designemos por $\mathfrak{J}_a$ la familia de ideales a la derecha de A , por $\mathfrak{J}_g$ la de los ideales a la izquierda, y por $\mathfrak{J} = \mathfrak{J}_a \cap \mathfrak{J}_g$ la de los ideales biláteros. Cada una de las familias $\mathfrak{J}_a, \mathfrak{J}_g, \mathfrak{J}$ es una familia de Moore, pues la intersección de dos familias de Moore de partes de A es una familia de Moore, y nosotros sabemos, de una parte que los subgrupos de un grupo forman una tal familia y, de otra, que las partes lícitas (o lícitas a un solo lado) con respecto a cualquier ley de composición la forman también. Designando por $\mathcal{S}$ la familia de Moore de subanillos de A , y por $\mathcal{C}$ la de los subgrupos aditivos, tendremos:

$$\mathfrak{J} \subseteq \mathfrak{J}_a \subseteq \mathcal{S} \subseteq \mathcal{C}, \quad \mathfrak{J} \subseteq \mathfrak{J}_g \subseteq \mathcal{S} \subseteq \mathcal{C}.$$

Cada una de las familias $\mathcal{I}, \mathcal{I}_a, \mathcal{I}_g$ está ordenada por la inclusión de conjuntos; cuando dos ideales de una misma familia verifican la relación de inclusión $\mathfrak{m} \subseteq \mathfrak{m}'$, se dice que $\mathfrak{m}$ es un *subideal* (o, también, un múltiplo) de $\mathfrak{m}'$, y que $\mathfrak{m}'$ es un *superideal* (o divisor) de $\mathfrak{m}$.

Las familias de Moore $\mathcal{I}_g, \mathcal{I}_a, \mathcal{I}$ están contenidas en la familia de Moore $\mathcal{C}$ de los subgrupos aditivos de A . Sea $\mathcal{F}$ una familia (finita o infinita) de ideales a la izquierda, por ejemplo $\mathcal{F} \subseteq \mathcal{I}_g \subseteq \mathcal{C}$. A esta familia $\mathcal{F}$ viene asociada la *intersección*, en el sentido de la teoría de conjunto de los ideales de $\mathcal{F}$: Esta intersección $\mathfrak{i} = \bigcap_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m}$ es el *máximo ideal contenido en cada ideal $\mathfrak{m}$ de la*

familia $\mathcal{F}$.

El mínimo ideal a la izquierda $\mathfrak{s}$ que contiene a cada uno de los ideales $\mathfrak{m}$ de la familia $\mathcal{F}$ viene caracterizado por el teorema que sigue.

Teorema 5. — *El mínimo subgrupo aditivo H del anillo A que contiene a cada ideal de una familia $\mathcal{F}$ de ideales a la izquierda es un ideal a la izquierda: $\mathfrak{s} = H$.*

El grupo H , suma de los ideales $\mathfrak{m}$ de $\mathcal{F}$ considerados como grupos aditivos, es, según sabemos, el conjunto de sumas finitas (con un número k de sumandos variable)

$$h = m_1 + \dots + m_k, \quad m_i \in \mathfrak{m}_i, \mathfrak{m}_i \in \mathcal{F}$$

formadas con elementos tomados en los subgrupos de la familia $\mathcal{F}$. Ahora bien, para todo elemento x de A tenemos

$$xh = xm_1 + \dots + xm_k \quad \text{y} \quad xm_i \in \mathfrak{m}_i$$

luego $xh \in H$, y H es, efectivamente, un ideal a la izquierda.

El mínimo ideal a la izquierda $\mathfrak{s} = H$ que contiene a cada ideal a la izquierda $\mathfrak{m}$ de la familia $\mathcal{F}$ es, por definición, la *suma* de los ideales $\mathfrak{m}$; se escribe

$$\mathfrak{s} = \sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m}$$

y, para una familia de dos ideales $\mathfrak{m}_1, \mathfrak{m}_2$ se pone:

$$\mathfrak{s} = \mathfrak{m}_1 + \mathfrak{m}_2.$$

La adición definida de este modo en $\mathfrak{I}_g$ es la restricción a $\mathfrak{I}_g$ de la adición de los subgrupos aditivos (adición de $\mathfrak{G}$); resulta *asociativa, conmutativa e idempotente*.

Del mismo modo se define la adición en $\mathfrak{I}_a$ y en $\mathfrak{I}$. una suma de ideales biláteros coincide con la suma de esos ideales considerados como ideales a la izquierda o a la derecha.

Puesto que el conjunto $\mathfrak{I}_g$ de los ideales a la izquierda de un anillo A es una familia de Moore, a cualquier parte no vacía B de A viene asociado un *mínimo ideal a la izquierda que contiene a B* , designado por $\widehat{B}_g$, y al que se llama ideal a la izquierda *engendrado* por B . La aplicación $B \rightarrow \widehat{B}_g$ en el conjunto de partes de A es una *clausura de Moore*, estrechamente ligada, por el teorema siguiente, a la clausura de Moore $X \rightarrow \overline{X}$ que asocia a cada parte no vacía X el mínimo subgrupo aditivo $\overline{X}$ que la contiene.

Teorema 6. — a) El ideal a la izquierda $\widehat{B}_g$ engendrado por B en el anillo A es el subgrupo aditivo engendrado por $B \cup AB$:

$$\widehat{B}_g = \overline{B \cup AB};$$

simétricamente, el ideal $\widehat{B}_a$ engendrado por B está dado por

$$\widehat{B}_a = \overline{B \cup BA}.$$

b) El ideal bilátero $\widehat{B}$ engendrado por B está dado por

$$\widehat{B} = \overline{B \cup AB \cup BA \cup ABA}.$$

c) Si el anillo A tiene un elemento unidad e , las fórmulas precedentes se transforman en

$$\widehat{B}_g = \overline{AB}, \quad \widehat{B}_a = \overline{BA}, \quad \widehat{B} = \overline{ABA}.$$

a) Cualquier elemento de $B \cup AB$ pertenece al ideal a la izquierda $\widehat{B}_g$, lo que da $\overline{B \cup AB} \subseteq \widehat{B}_g$. Recíprocamente el grupo aditivo $\overline{B \cup AB}$ es el conjunto de sumas finitas formadas con los elementos de $B \cup (-B)$ o de AB :

$$h = b'_1 + \dots + b'_r + a_1 b_1 + \dots + a_s b_s, \quad a_i \in A; b_i \in B, b'_j \in B \cup (-B)$$

para todo elemento x de A tendremos

$$xh = xb'_1 + \dots + xb'_r + xa_1 b_1 + \dots + xa_s b_s \in \overline{AB} \subseteq \overline{B \cup AB},$$

luego $\overline{B \cup AB}$ es lícito multiplicativamente a la izquierda, y es un ideal a la izquierda que contiene a B , lo que implica $\widehat{B}_g \subseteq \overline{B \cup AB}$, de donde se tiene la igualdad.

b) Tenemos análogamente

$$R = B \cup AB \cup BA \cup ABA \subseteq \widehat{B}$$

luego $\overline{R} \subseteq \widehat{B}$. Si un elemento

$$h = \sum_{\lambda} b_{\lambda}''' + \sum_{\mu} a_{\mu}'' b_{\mu}'' + \sum_{\nu} b_{\nu}' a_{\nu}' + \sum_{\rho} a_{\rho} b_{\rho} a_{\rho}^* \in \overline{R}$$

(las sumas son finitas, las a son elementos de A , y las b de B) lo multiplicamos a la izquierda o a la derecha por un elemento cualquiera de A , obtenemos un elemento de $\overline{AB \cup BA \cup ABA} \subseteq \overline{R}$, luego $\overline{R}$ es multiplicativamente lícito. Es $\overline{R}$ un ideal bilátero que incluye a B , lo que implica $\widehat{B} \subseteq \overline{R}$ y, por esto vale el signo igual.

c) Si el anillo A tiene elemento unidad e , tendremos

$$B = eB \subseteq AB = ABe \subseteq ABA$$

$$B = Be \subseteq BA = eBA \subseteq ABA$$

luego

$$B \cup AB = AB, \quad B \cup BA = BA, \quad B \cup AB \cup BA \cup ABA = ABA,$$

y resultan las fórmulas del enunciado.

Casos particulares. — 1. Supongamos que B sea una parte lícita a la izquierda, en cuyo caso $AB \subseteq B$, luego $\widehat{B}_g = \overline{B}$; el ideal a la izquierda engendrado por una parte lícita a la izquierda B coincide con el subgrupo aditivo engendrado por B .

Del mismo modo, si B es una parte lícita, tendremos $AB \subseteq B$, $BA \subseteq B$, $ABA \subseteq B$ y el ideal bilátero engendrado por una parte lícita B coincide con el subgrupo aditivo engendrado por B : $\widehat{B} = \overline{B}$.

2. Cuando B viene dado en forma de unión de conjuntos, $B = B_1 \cup B_2$, se tiene, para los ideales biláteros engendrados por B , B_1 , B_2 :

$$(1) \quad \widehat{B} = \widehat{B_1 \cup B_2} = \widehat{B_1} + \widehat{B_2}$$

y lo mismo para los ideales a la izquierda o a la derecha. En efecto la fórmula establecida en general para una clausura de Moore (Cap. I, § 4, ejemplo 1) da en este caso

$$\widehat{B_1 \cup B_2} = \widehat{B_1} \cup \widehat{B_2}$$

y el ideal del segundo miembro, engendrado por la unión de los ideales $\widehat{B_1}$, $\widehat{B_2}$, es el mínimo ideal que los incluye, es decir su suma $\widehat{B_1} + \widehat{B_2}$.

3. Si el conjunto de generadores B tiene un solo elemento, $B = \{b\}$, el ideal a la izquierda $\widehat{B}_g$ se llama *principal a la izquierda* y se designa por $(b)_g$; es el conjunto de los elementos $\nu b + rb$ ($\nu \in \mathbb{Z}$, $r \in A$), que se llama *múltiplos a la izquierda* de b en A .

Cuando A tiene un elemento unidad e , $\widehat{B}_g$ es el conjunto de elementos ab ($a \in A$); según el teorema 6; también se puede destacar que entonces tenemos $\nu b + rb = (\nu e + r)b$, donde $\nu e + r \in A$.

El ideal a la derecha $\widehat{B}_d$ engendrado por $B = \{b\}$ se llama *principal a la derecha*, y se indica por $\{b\}$; lo constituye el conjunto de los *múltiplos a la derecha*.

$$\nu b + br \quad (\nu \in \mathbb{Z}, r \in A)$$

o, si A contiene un elemento unidad, de los productos ab ($a \in A$).

El ideal bilátero $\widehat{B}$ engendrado por b se llama *principal*. Aquí la suma de dos elementos rbr' , $r_1br'_1$ con $r, r', r_1, r'_1 \in A$, no es ya un elemento de esa forma.

4. Cuando un ideal (a la izquierda, por ejemplo) de un anillo A está engendrado por un conjunto *finito* $B = \{b_1, \dots, b_k\}$, se dice que admite una *base finita* B (en teoría de ideales la palabra *base* designa a un conjunto de generadores sin hacer la hipótesis de que sea irreducible, de modo que puede contener estrictamente a otro).

Si se trata, por ejemplo, de un ideal a la izquierda, $\mathfrak{g}$, se escribe

$$\mathfrak{g} = (b_1, \dots, b_k)$$

y se tiene, según la fórmula (1),

$$\mathfrak{g} = \sum_{i=1}^k (b_i);$$

la suma de dos ideales a la izquierda que admiten bases finitas, $\mathfrak{g} = (b_1, \dots, b_k)$,

$\mathfrak{g}' = (b'_1, \dots, b'_{k'})$ admite también una base finita, y esta es la unión de las bases de $\mathfrak{g}$ y $\mathfrak{g}'$:

$$\mathfrak{g} + \mathfrak{g}' = (b_1, \dots, b_k, b'_1, \dots, b'_{k'}).$$

Demos un *ejemplo de investigación de una base* para un ideal dado. Sean: A un anillo conmutativo con elemento unidad, $P_n = A[x_1, \dots, x_n]$ el anillo de los polinomios en $x_1, \dots, x_n$ con coeficientes en A , $(a_1, \dots, a_n)$ un punto del espacio A^n , y $\mathfrak{m}$ el ideal de los polinomios $f \in P_n$ nulos en ese punto.

Consideremos el ideal

$$\mathfrak{m}' = (x_1 - a_1, \dots, x_n - a_n)$$

Todo polinomio $x_i - a_i$ de la base de $\mathfrak{m}'$ se anula en el punto $(a_1, \dots, a_n)$, y por lo tanto pertenece a $\mathfrak{m}$; así resulta $\mathfrak{m}' \subseteq \mathfrak{m}$.

Pero, recíprocamente, como la equivalencia $\mathcal{R}'$ asociada al ideal $\mathfrak{m}'$ es compatible con la adición y la multiplicación, las congruencias

$$x_i \equiv a_i (\mathfrak{m}')$$

implican, para cualquier polinomio $f \in P_n$,

$$f(x_1, \dots, x_n) \equiv f(a_1, \dots, a_n) \quad (\mathfrak{m}')$$

es decir,

$$f(x_1, \dots, x_n) = f(a_1, \dots, a_n) + h_1(x_1 - a_1) + \dots + h_n(x_n - a_n)$$

con $h_\nu \in P_n$ ($\nu = 1, 2, \dots, n$).

Establecido esto, si $f \in \mathfrak{m}$, se tiene $f(a_1, \dots, a_n) = 0$, luego $f(x_1, \dots, x_n) \in \mathfrak{m}'$, de donde $\mathfrak{m} \subseteq \mathfrak{m}'$ y, por consiguiente, $\mathfrak{m} = \mathfrak{m}'$.

De este modo, en el anillo $P_n = A[x_1, \dots, x_n]$, donde A indica un anillo conmutativo con elemento unidad, el ideal $\mathfrak{m}$ de los polinomios nulos en el punto $(a_1, \dots, a_n)$ es el ideal

$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n).$$

En particular, para $n = 1$, en el anillo $P_1 = A[x]$, el ideal de los polinomios nulos para $x = a$, ($a \in A$), es el ideal principal $(x - a)$.

En un anillo cualquiera A sabemos definir, a partir de la multiplicación de elementos, la multiplicación de partes (no vacías).

$$XY = \{xy; x \in X, y \in Y\}$$

y luego, a partir de ésta, la multiplicación $\dashv$ en cualquier familia de Moore $\mathcal{F}$:

$$F_1 \dashv F_2 = \overline{F_1 F_2} \quad (F_1, F_2 \in \mathcal{F})$$

(cap. I, § 4, 5.º). Este procedimiento se aplica, en particular, a las familias de Moore $\mathcal{J}_g$ de los ideales a la izquierda, $\mathcal{J}_d$ de los ideales a la derecha, e $\mathcal{J}$ de los ideales biláteros.

En $\mathcal{J}_g$ por ejemplo, el producto $\mathfrak{m} \dashv \mathfrak{m}'$ de los ideales a la izquierda $\mathfrak{m}$ y $\mathfrak{m}'$ es el ideal a la izquierda $\widehat{B_g}$ engendrado por la parte B , conjunto de productos mm' con $m \in \mathfrak{m}$, y $m' \in \mathfrak{m}'$. Pero B es una parte lícita a la izquierda y, según el teor. 6 (caso particular 1.º), el ideal $\widehat{B_g}$ no es otra cosa que el grupo aditivo $\overline{B}$ engendrado por B , esto es, el conjunto de las sumas finitas $m_1 m'_1 + \dots + m_k m'_k$ ($k \in \{1, 2, \dots\} = N$, $m_i \in \mathfrak{m}$, $m'_i \in \mathfrak{m}'$). A este conjunto de sumas finitas

$$\sum_{i=1}^k m_i m'_i, \quad (k \in N, m_i \in \mathfrak{m}, m'_i \in \mathfrak{m}').$$

le llamaremos, pues, ideal producto de los $\mathfrak{m}$ y $\mathfrak{m}'$ y es, efectivamente, un ideal a la izquierda.

Este ideal producto lo indicaremos, por simplicidad, con la notación $\mathfrak{m}\mathfrak{m}'$, en vez de $\mathfrak{m} \dashv \mathfrak{m}'$; por lo demás el empleo de letras góticas quita todo riesgo de confusión.

Se extiende esta definición a la multiplicación de ideales por la derecha y a la de ideales biláteros.

Observaciones. — 1. La definición de ideal producto $\mathfrak{m}\mathfrak{m}'$ de dos ideales a la izquierda se aplica también aunque se reemplace $\mathfrak{m}'$ por una parte cualquiera no vacía C del anillo A . El ideal producto $\mathfrak{m}C$ es el ideal a la izquierda conjunto de las sumas finitas

$$\sum_{i=1}^k m_i c_i, \quad (k \in N, m_i \in \mathfrak{m}, c_i \in C).$$

Se tiene una propiedad simétrica para los ideales a la derecha, pero esta extensión cae en defecto para los ideales biláteros.

2. Si el anillo A tiene elemento unidad e , el ideal a la izquierda $\widehat{B}_g = \overline{AB}$ engendrado por una parte no vacía B , no es otra cosa que el ideal producto del ideal unidad $(e) = A$ por la parte B .

La multiplicación de ideales a la izquierda es *asociativa*: $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$; el producto de un número finito de ideales a la izquierda en un orden dado queda, pues, definido de un modo único, y se puede hablar de potencias $\mathfrak{m}^a$ de un ideal a la izquierda $\mathfrak{m}$ para cualquier entero positivo a .

Se define simétricamente el ideal producto $C\mathfrak{a}$ de una parte no vacía C por un ideal a la derecha $\mathfrak{a}$; es un ideal a la derecha. La multiplicación así definida en el conjunto $\mathfrak{I}_d$ de los ideales a la derecha es asociativa.

El producto $\mathfrak{g}\mathfrak{d}$ de un ideal a la izquierda $\mathfrak{g}$ por un ideal a la derecha $\mathfrak{d}$ es lo mismo si se considera como producto del ideal a la izquierda $\mathfrak{g}$ por la parte $\mathfrak{d}$ (y entonces es un ideal a la izquierda) o como producto del ideal a la derecha $\mathfrak{d}$ por la parte $\mathfrak{g}$ (y entonces es un ideal a la derecha). Este producto $\mathfrak{g}\mathfrak{d}$ es, por lo tanto, un ideal bilátero.

Esta multiplicación de los ideales a la izquierda por los ideales a la derecha, que tiene por resultado un ideal bilátero, es una ley de composición de forma general, a saber, una aplicación de $\mathfrak{I}_g \times \mathfrak{I}_d$ en $\mathfrak{I}$. La multiplicación de ideales biláteros es un caso particular, que da, en $\mathfrak{I}$, una ley de composición interna asociativa.

Si $\mathfrak{g}$ admite una base finita G , $\mathfrak{g} = \overline{G \cup AG}$, y si $\mathfrak{d}$ admite una base finita D , $\mathfrak{d} = \overline{D \cup DA}$, el ideal producto $\mathfrak{g}\mathfrak{d}$ es el subgrupo aditivo de A engendrado por los productos xy , $x \in \mathfrak{g}$, $y \in \mathfrak{d}$. Como x es suma finita de elementos de $G \cup AG$ e y es suma finita de elementos de $D \cup DA$, xy viene a ser suma finita de elementos de $(G \cup AG)(D \cup DA)$ y tendremos

$$\begin{aligned}\mathfrak{g}\mathfrak{d} &= \overline{(G \cup AG)(D \cup DA)} \\ &= \overline{GD \cup AGD \cup GDA \cup AGDA}\end{aligned}$$

lo que, teniendo en cuenta el teor. 6, demuestra que $\mathfrak{g}\mathfrak{d}$ admite la base finita GD . Si

$$G = \{g_1, \dots, g_h\}, \quad D = \{d_1, \dots, d_k\},$$

tendremos

$$GD = \{g_1d_1, \dots, g_id_j, \dots, g_hd_k\}$$

y para los ideales

$$(2) \quad (g_1, \dots, g_h) \{d_1, \dots, d_k\} = (g_1 d_1, \dots, g_1 d_k, \dots, g_h d_1, \dots, g_h d_k).$$

Si $\mathfrak{g}$ y $\mathfrak{d}$ son principales, $\mathfrak{gd}$ es principal.

En el conjunto $\mathfrak{I}_\theta$ de los ideales a la izquierda, por ejemplo, no son válidas las propiedades precedentes; el producto de dos ideales principales a la izquierda $(\mathfrak{g})$ y $(\mathfrak{g}')$ no contiene solamente a gg' , y a los elementos de la forma agg' ($a \in A$), sino también los elementos $aga'g'$ y las sumas de tales elementos. Así, $(\mathfrak{g})(\mathfrak{g}')$ contiene a (gg') sin serle, en general, igual.

La multiplicación de ideales a la izquierda, por ejemplo, es *isótoma* (o, como también se dice, *respeto la relación de inclusión*), es decir:

$$\mathfrak{g} \subseteq \mathfrak{g}' \quad \text{implica} \quad \mathfrak{gg}_1 \subseteq \mathfrak{g}'\mathfrak{g}_1 \quad \text{y} \quad \mathfrak{g}_1\mathfrak{g} \subseteq \mathfrak{g}_1\mathfrak{g}'$$

cualesquiera sean $\mathfrak{g}, \mathfrak{g}', \mathfrak{g}_1 \in \mathfrak{I}_\theta$. Sean $\mathcal{F}$ una familia de ideales a la izquierda, $\mathfrak{m}$ un ideal en $\mathcal{F}$ y $\mathfrak{a}$ la suma

$$\mathfrak{a} = \sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m}.$$

La inclusión $\mathfrak{m} \subseteq \mathfrak{a}$ implica $\mathfrak{gm} \subseteq \mathfrak{ga}$ para todo $\mathfrak{m} \in \mathcal{F}$, de donde

$$\sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{gm} \subseteq \mathfrak{g} \left(\sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m} \right).$$

Inversamente, $\mathfrak{ga}$ es el grupo aditivo engendrado por el conjunto de productos gx en los que x , elemento de $\mathfrak{a}$, es de la forma

$$x = m_1 + \dots + m_k, \quad m_i \in \mathfrak{m}_i, \quad \mathfrak{m}_i \in \mathcal{F},$$

de donde

$$gx = gm_1 + \dots + gm_k \in \sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{gm}$$

En consecuencia tendremos

$$\mathfrak{g} \left(\sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m} \right) \subseteq \sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{gm}$$

y, finalmente, la igualdad,

$$\mathfrak{g} \left(\sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m} \right) = \sum_{\mathfrak{m} \in \mathcal{F}} \mathfrak{g}\mathfrak{m}.$$

Esta igualdad expresa la *distributividad a la izquierda* de la multiplicación con respecto a la adición en $\mathfrak{J}_g$, pero resulta válida para la suma de una familia $\mathcal{F}$ finita o infinita, por lo que diremos que se tiene aquí la *propiedad distributiva general*. Del mismo modo se establece, en $\mathfrak{J}_g$, la distributividad general a la derecha de la multiplicación con respecto a la adición; y se tienen las mismas propiedades en $\mathfrak{J}_a$, y en $\mathfrak{J}$ para la multiplicación de los ideales a la izquierda por los ideales a la derecha ¹.

La relación

$$\bigcap_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m} \subseteq \mathfrak{m}$$

implica

$$\begin{aligned} \mathfrak{g} \left(\bigcap_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m} \right) &\subseteq \bigcap_{\mathfrak{m} \in \mathcal{F}} \mathfrak{g}\mathfrak{m} \\ \left(\bigcap_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m} \right) \mathfrak{g} &\subseteq \bigcap_{\mathfrak{m} \in \mathcal{F}} \mathfrak{m}\mathfrak{g} \end{aligned}$$

pero aquí *la igualdad no se verifica en general*, como hacen ver ejemplos análogos al siguiente.

Ejemplo. — Consideremos el anillo $P = \mathbf{R}[x, y, z, t]$ de polinomios en x, y, z, t , de coeficientes reales, por ejemplo, y en este anillo los ideales

$$\mathfrak{a} = (y, z), \quad \mathfrak{m} = (x, y), \quad \mathfrak{m}' = (z, t).$$

Sea $F = Ax + By = Cz + Dt$, $A, B, C, D \in P$, un polinomio de la intersección $\mathfrak{m} \cap \mathfrak{m}'$. La sustitución $z = t = 0$ da

$$A(x, y, 0, 0)x + B(x, y, 0, 0)y = 0$$

de donde

$$A = Qy + A_1z + B_1t, \quad B = -Qx + A_2z + B_2t$$

¹ Utilizando el carácter distributivo de la multiplicación de ideales respecto a la suma, y el hecho inmediato de que el producto de un ideal principal a la izquierda por un ideal principal a la derecha es un ideal principal bilátero, se obtiene fácilmente una segunda demostración de la fórmula (2).

$(Q, A_i, B_i \in P)$ y estas igualdades implican

$$F \in (x, y) (z, t) = \mathfrak{m}\mathfrak{m}'$$

Tendremos, pues,

$$\mathfrak{m} \cap \mathfrak{m}' \subseteq \mathfrak{m}\mathfrak{m}' \subseteq \mathfrak{m} \cap \mathfrak{m}'$$

de donde la igualdad, que implica

$$\mathfrak{a}(\mathfrak{m} \cap \mathfrak{m}') = (y, z) (x, y) (z, t)$$

con lo que el ideal $\mathfrak{a}(\mathfrak{m} \cap \mathfrak{m}')$ no contiene ningún monomio de grado menor que 3.

Por otra parte tenemos

$$\mathfrak{a}\mathfrak{m} = (y, z) (x, y)$$

$$\mathfrak{a}\mathfrak{m}' = (y, z) (z, t)$$

y por lo tanto $yz \in \mathfrak{a}\mathfrak{m} \cap \mathfrak{a}\mathfrak{m}'$, mientras que $yz \notin \mathfrak{a}(\mathfrak{m} \cap \mathfrak{m}')$. La inclusión

$$\mathfrak{a}(\mathfrak{m} \cap \mathfrak{m}') \subset \mathfrak{a}\mathfrak{m} \cap \mathfrak{a}\mathfrak{m}'$$

es, pues, estricta.

§ 8. Ideales maximales. Ideales primos

Sea $\mathfrak{m}$ un ideal en un anillo conmutativo A .

Estudiemos las propiedades del anillo cociente $A/\mathfrak{m}$ y estudiemos, principalmente, cuando $A/\mathfrak{m}$ es un cuerpo o, más generalmente, un dominio de integridad.

Definición. — Un ideal *maximal* (o *sin divisores*)¹ del anillo A es un ideal $\mathfrak{m}$ que no tiene más superideales (o divisores) que A y él mismo:

$$\mathfrak{m} \subset \mathfrak{m}' \subseteq A \quad \text{implica} \quad \mathfrak{m}' = A.$$

¹ También se le llama ideal *divisor mínimo*. (N. del T.)

El nombre se justifica porque tal ideal es maximal en el conjunto $\mathfrak{J} - \{A\} = \mathfrak{J}'$ de los ideales propios de A , es decir, que no está contenido en ningún otro ideal de ese conjunto.

Teorema 1. — 1.º Para que el anillo cociente $A/\mathfrak{m}$ sea un cuerpo, es necesario que $\mathfrak{m}$ sea maximal.

2.º Si A tiene elemento unidad, e , y si $\mathfrak{m}$ es ideal maximal, el cociente $A/\mathfrak{m}$ es un cuerpo.

1.º Supongamos que $A/\mathfrak{m}$ sea un cuerpo, y sea $\mathfrak{m}'$ un ideal de A con la condición

$$\mathfrak{m} \subset \mathfrak{m}' (\subseteq A)$$

Existe un elemento $c \notin \mathfrak{m}$ y $c \in \mathfrak{m}'$; la clase C módulo $\mathfrak{m}$ a la que pertenece c es distinta de la clase cero, es decir, de $\mathfrak{m}$. Si x es un elemento cualquiera de A , situado en la clase X , existe una clase C' tal que

$$X = CC'$$

y, si $c' \in C'$, se tiene

$$x \equiv cc'(\mathfrak{m}),$$

es decir

$$x = cc' + m \quad \text{donde} \quad m \in \mathfrak{m} \subset \mathfrak{m}', \quad \text{y} \quad c \in \mathfrak{m}',$$

luego $cc' \in \mathfrak{m}'$, de donde $x \in \mathfrak{m}'$ y $\mathfrak{m}' = A$, como queríamos demostrar.

2.º Supongamos que A tiene un elemento unidad e , y que $\mathfrak{m}$ sea un ideal maximal. Para probar que $A/\mathfrak{m}$ es un cuerpo demostraremos que cualquiera que sea $X \in A/\mathfrak{m}$ y $C \in A/\mathfrak{m}$ distinto de la clase cero, $\mathfrak{m}$, existe una clase C' tal que $CC' = X$.

Sea $c \in C$; $c \notin \mathfrak{m}$; por lo tanto $\mathfrak{m} \subset \mathfrak{m} + (c)$ (estrictamente), luego

$$\mathfrak{m} + (c) = A.$$

Si $x \in X$, se tiene, según la igualdad precedente,

$$x = m + y \quad \text{donde} \quad m \in \mathfrak{m} \quad \text{y donde} \quad y \in (c),$$

ahora bien, A tiene elemento unidad, lo que implica $(c) = Ac$; luego $y = c'c$. De este modo

$$x = m + c'c, \quad \text{con} \quad m \in \mathfrak{m}$$

de donde, designando por C' la clase que contiene a c' ,

$$X = 0 + C'C = C'C \quad \text{c.q.d.}$$

Observación. — La hipótesis de la existencia de elemento unidad en el anillo es indispensable para la segunda parte del teorema. Lo manifiesta así, por ejemplo, el caso del anillo A de los números pares, en donde el ideal $\mathfrak{m} = (4)$ es claramente maximal [si $c \notin \mathfrak{m}$, $\mathfrak{m} + (c) = A$]. En el anillo cociente $A/(4) = \{\bar{0}, \bar{2}\}$ es $\bar{2}^2 = \bar{0}$. Y como este anillo tiene divisores de cero no puede ser un campo.

Definición. — Un ideal $\mathfrak{p}$ de un anillo A se llama *ideal primo*, por definición, cuando el anillo cociente $A/\mathfrak{p}$ es un dominio de integridad. Para esto es necesario y suficiente que, designando por $\bar{0} = \mathfrak{p}$ el elemento cero del anillo cociente $A/\mathfrak{p}$, y por X, Y dos cualesquiera de sus clases, *sean incompatibles* las relaciones

$$XY = \bar{0}, \quad X \neq \bar{0}, \quad Y \neq \bar{0}$$

Esto se traduce, volviendo a los elementos del anillo A , en que *sean incompatibles* las relaciones

$$xy \in \mathfrak{p}, \quad x \notin \mathfrak{p}, \quad y \notin \mathfrak{p}$$

Esta condición se suele expresar de una de las dos formas siguientes:

- a) $xy \in \mathfrak{p}$, y $x \notin \mathfrak{p}$ implican $y \in \mathfrak{p}$;
- b) $x \notin \mathfrak{p}$ e $y \notin \mathfrak{p}$ implican $xy \notin \mathfrak{p}$;

o, en otros términos, el conjunto complementario $A - \mathfrak{p}$ es estable para la multiplicación. Recíprocamente, si el complementario $A - \mathfrak{p}$ de un ideal $\mathfrak{p}$ es multiplicativamente estable, este ideal es primo.

Se puede en la condición a) por ejemplo, reemplazar los elementos por los ideales, y el signo $\in$ por el signo $\subseteq$:

a') Para que un ideal $\mathfrak{p}$ sea primo, es necesario y suficiente que las relaciones

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \quad \mathfrak{a} \not\subseteq \mathfrak{p}$$

impliquen

$$\mathfrak{b} \subseteq \mathfrak{p}$$

(siendo $\mathfrak{a}$, y $\mathfrak{b}$, dos ideales del anillo A).

Supongamos en efecto que $\mathfrak{p}$ verifica la condición a'). Si $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ y $\mathfrak{a} \not\subseteq \mathfrak{p}$, poniendo $\mathfrak{a} = (a)$, y $\mathfrak{b} = (b)$, se tiene $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, $\mathfrak{a} \not\subseteq \mathfrak{p}$, luego $\mathfrak{b} \subseteq \mathfrak{p}$ y $b \in \mathfrak{p}$: la condición a) queda satisfecha por $\mathfrak{p}$.

Recíprocamente, si $\mathfrak{p}$ cumple la condición a) y si se tiene $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, $\mathfrak{a} \not\subseteq \mathfrak{p}$, sea a un elemento de $\mathfrak{a}$ no situado en $\mathfrak{p}$; cualquiera que sea $b \in \mathfrak{b}$, tenemos $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ y como $a \notin \mathfrak{p}$, resulta $b \in \mathfrak{p}$, luego $\mathfrak{b} \subseteq \mathfrak{p}$.

El mismo anillo A es un ideal primo, como se ve aplicando la condición a). Para que el ideal (0) sea primo es necesario y suficiente que A sea un dominio de integridad: se tiene, en efecto $A/(0) \simeq A$.

Según el teorema 1, todo ideal maximal en un anillo A con elemento unidad es primo, pues todo cuerpo es un dominio de integridad.

Recíprocamente, si $\mathfrak{p}$ es primo y si $A/\mathfrak{p}$ es finito, $A/\mathfrak{p}$, por ser dominio de integridad finito es un cuerpo, luego $\mathfrak{p}$ es maximal.

Ejemplos. — 1. En el anillo $\mathbb{Z}$ de los enteros, como todo anillo cociente $A/(m) = \{\bar{0}, \bar{1}, \dots, \bar{m-1}\}$ ($m \neq 0$) es finito, y como $A/(m)$ es un dominio de integridad y por ende un cuerpo, si, y sólo si, m es un número primo p , resulta: los ideales primos no nulos de $\mathbb{Z}$ son los ideales engendrados por un número primo (p), y son maximales.

En cuanto al ideal (0) en $\mathbb{Z}$, es primo pero no es maximal.

2. Sean A un anillo conmutativo con elemento unidad $P_n = A[x_1, \dots, x_n]$ el anillo de los polinomios en $x_1, \dots, x_n$ con coeficientes en A , $(a_1, \dots, a_n)$ un punto del espacio A^n , y

$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$$

el ideal de los polinomios f de P_n nulos en este punto (ver § 7).

La aplicación

$$(a) \quad f(x_1, \dots, x_n) \rightarrow f(a_1, \dots, a_n)$$

de P_n en A es exhaustiva, pues todo elemento a de A es imagen del polinomio a de P (polinomio de grado nulo).

Además esta aplicación es un *homomorfismo* de anillos (pues respeta la adición y la multiplicación de P_n y de A) y el núcleo de este homomorfismo α , conjunto de polinomios nulos en el punto $(a_1, \dots, a_n)$, es el ideal $\mathfrak{m}$. Se tiene, pues, según el teorema del homomorfismo, el isomorfismo

$$P_n/\mathfrak{m} \simeq A.$$

Luego: Si A es un dominio de integridad con elemento unidad, el ideal $\mathfrak{m}$, en P_n , es primo; si A es un cuerpo, el ideal $\mathfrak{m}$, en P_n , es maximal y, a fortiori, primo.

3. Designando por Ω el cuerpo de los complejos, consideremos el anillo $A = \Omega[x, y, z]$ y los ideales de A siguientes:

$\mathfrak{m} = (x, y, z)$, ideal de los polinomios nulos en el origen; es maximal, según el ejemplo precedente, luego es primo.

$\mathfrak{p}_1 = (x, y)$. Toda clase C módulo $\mathfrak{p}_1$ contiene un polinomio $\varphi(z) \in \Omega[z]$ y sólo uno, resultado común de la sustitución $x = y = 0$ en los polinomios de C . Las clases C se suman y multiplican como sus representantes $\varphi(z)$ y tenemos por eso el isomorfismo

$$A/\mathfrak{p}_1 \simeq \Omega[z],$$

y $\Omega[z]$ es un dominio de integridad, luego $\mathfrak{p}_1$ es un ideal primo de A .

$\mathfrak{p}_2 = (x)$; se puede hacer un razonamiento análogo, considerando para cada clase módulo $\mathfrak{p}_2$, un representante $\psi(y, z) \in \Omega[y, z]$. Aquí se tiene

$$A/\mathfrak{p}_2 \simeq \Omega[y, z],$$

$\Omega[y, z]$ es un dominio de integridad y, por lo tanto, el ideal $\mathfrak{p}_2$ es primo en A .

Se tiene así la cadena creciente (finita) de ideales primos

$$\mathfrak{p}_2 \subset \mathfrak{p}_1 \subset \mathfrak{m} \subset A$$

y $\mathfrak{p}_1, \mathfrak{p}_2$ son, según esto, ideales primos no maximales.

4. Consideremos el anillo $\mathcal{S}$ de las sucesiones $\{x_i\}$ de números reales, $x_i \in \mathbf{R}$ la adición y la multiplicación se realizan "término a término".

Las sucesiones se dicen acotadas cuando existen un número H y un entero N tales que para $n \geq N$ sea $|x_i| < H$. El conjunto $\mathcal{B}$ de las sucesiones acotadas es un subanillo de $\mathcal{S}$.

El conjunto $\mathcal{C}$ de las sucesiones convergentes es un subanillo de $\mathcal{B}$ y de $\mathcal{S}$ según la teoría elemental de límites.

El conjunto $\mathcal{J}$ de las sucesiones *nulas*, es decir, de límite 0, es subanillo de $\mathcal{C}$ de $\mathcal{B}$, y de $\mathcal{S}$.

El conjunto $\mathcal{J}_0$ de las sucesiones *nulas triviales*, es decir, con todos los $x_i = 0$ a partir de cierto lugar i de orden (no determinado) es subanillo de los antedichos.

Finalmente, el conjunto $\mathcal{J}_k$ de las sucesiones que tienen nulos todos sus términos a partir de un índice k ($x_i = 0$ para $i > k$) es un subanillo de los antedichos, y también $\mathcal{J}_{k+1}, \dots$; Así tenemos:

$$\mathcal{J}_0 \subset \dots \subset \mathcal{J}_k \subset \dots \subset \mathcal{J}_0 \subset \mathcal{J} \subset \mathcal{C} \subset \mathcal{B} \subset \mathcal{S}.$$

Como se ha visto antes, $\mathcal{J}_k$ es un ideal en $\mathcal{S}$ y por lo tanto en todos los anillos intermedios. Las $\mathcal{J}_k$ forman una cadena: su unión $\mathcal{J}_0$ es un ideal en $\mathcal{S}$, (luego también en los anillos intermedios $\mathcal{J}, \mathcal{C}, \mathcal{B}, \mathcal{S}$).

$\mathcal{J}_0$ no es primo en $\mathcal{J}$, luego tampoco lo es en $\mathcal{C}, \mathcal{B}, \mathcal{S}$. Tomemos, en efecto,

$$S_1 = \left\{ 1, 0, \frac{1}{2}, 0, \dots, \frac{1}{2^p - 1}, 0, \dots \right\}, \quad S_1 \notin \mathcal{J}_0, \quad S_1 \in \mathcal{J},$$

$$S_2 = \left\{ 0, \frac{1}{2}, 0, \frac{1}{4}, \dots, 0, \frac{1}{2^p}, \dots \right\}, \quad S_2 \notin \mathcal{J}_0, \quad S_2 \in \mathcal{J}$$

y obtenemos:

$$S_1 S_2 = \{ 0, 0, \dots, 0, 0, \dots \} \in \mathcal{J}_0$$

Tenemos también $S_1 S_2 \in \mathcal{J}_k \quad \forall k$, luego $\mathcal{J}_k$ no es primo en $\mathcal{J}$, ni en $\mathcal{C}, \mathcal{B}, \mathcal{S}$.

El conjunto $\mathcal{J}$ de las sucesiones nulas es un ideal maximal, luego primo, en el anillo $\mathcal{C}$ de las sucesiones convergentes.

$\mathcal{J}$ es primero, visiblemente, un ideal en $\mathcal{B}$, luego en $\mathcal{C}$.

Sea $\mathcal{M}$ un ideal de $\mathcal{C}$ tal que

$$\mathcal{J} \subset \mathcal{M} \subseteq \mathcal{C}$$

Estableceremos la igualdad $\mathcal{M} = \mathcal{C}$. Para ello sea $X \in \mathcal{C}$ y $\lim X = x$. Como $\mathcal{J} \neq \mathcal{M}$, existe una sucesión S tal que $S \in \mathcal{M}$, $S \notin \mathcal{J}$, luego $\lim S = s \neq 0$.

Consideremos la sucesión $T = \{t_i\}$ donde $t_i = x/s, \forall i; T \in \mathbb{C}$, $\lim T = x/s$ y se tiene

$$\lim (TS) = x/s \cdot s = x = \lim X$$

luego

$$\lim (X - TS) = 0, \quad \text{es decir} \quad X - TS \in \mathfrak{J} \subset \mathcal{M}$$

y como $S \in \mathcal{M}$, se tiene $X \in \mathcal{M}$, luego $\mathcal{M} = \mathbb{C}$.

En el subanillo $\mathcal{B}$ de las sucesiones acotadas el ideal $\mathfrak{J}$ no es primo.

Tomemos

$$S' = \{1, 0, 1, 0, \dots\} \notin \mathfrak{J}, S' \in \mathcal{B}$$

$$S'' = \{0, 1, 0, 1, \dots\} \notin \mathfrak{J}, S'' \in \mathcal{B};$$

Se tiene

$$S'S'' = \{0, 0, 0, 0, \dots\} \in \mathfrak{J}$$

Este ejemplo pone de relieve un hecho importante que, por lo demás, ya era claro en las definiciones: para un ideal, las propiedades de ser *máximo* y de ser *primo* son propiedades *relativas*, es decir, que no dependen sólo del ideal, sino también del anillo en que se considere. Si, por ejemplo, $\mathfrak{p}$ es ideal primo de A , y si A' y A'' son anillos tales que

$$\mathfrak{p} \subset A' \subset A \subset A''$$

$\mathfrak{p}$ es, ciertamente, ideal primo de A' pero puede no ser ideal primo de A'' , e incluso puede que no sea ni tan siquiera ideal de A'' . Así, el conjunto $\mathfrak{p}$ de los enteros pares, es ideal maximal en el anillo de los enteros, pero no es un ideal del anillo (cuerpo) de los números racionales.

CAPÍTULO V

CONJUNTOS ORDENADOS. RETÍCULOS

§ 1. Conjuntos ordenados. Cadenas

Un conjunto ordenado es un conjunto E en el cual se ha definido una *relación de orden*, es decir una relación binaria θ que cumple estas condiciones:

- 1.º *Reflexiva*: $a \theta a, \forall a \in E$;
- 2.º *Transitiva*: $a \theta b$ y $b \theta c$ implica $a \theta c$
- 3.º *Antisimétrica* (o *propia*): $a \theta b$ y $b \theta a$ implica $a = b$.

A menudo utilizaremos la notación $a \leq b$, que se lee: a es anterior a b , o precede a b , o es menor o igual a b . Se puede escribir también $b \geq a$. (b es posterior, o sigue, o es mayor o igual a a).

Si entre dos elementos se tiene: $a \leq b$ o $b \leq a$ se dice que son comparables. El no serlo se expresa con el símbolo $a \parallel b$.

La restricción de la relación de orden θ a un subconjunto E' de E es una relación de orden θ' : todo subconjunto de un conjunto ordenado es también conjunto ordenado.

Observaciones. — 1.º $a < b$ quiere decir que, simultáneamente, $a \leq b$ y $a \neq b$. Es también una relación binaria, que llamaremos *relación de orden estricto*. Es transitiva, y $a < b$ y $b < a$ son incompatibles.

2.º En un conjunto ordenado, la negación de $a < b$ es: $\{b \leq a \text{ o } a \parallel b\}$.

3.º Si, para todo par (a, b) de elementos de E se tiene $a \leq b$ o $b \leq a$, el conjunto se dice totalmente ordenado, o, también, *cadena*. En este caso escribiremos $a \leq b$ con preferencia a $a \leq b$.

4.º *Parte hereditaria* de un conjunto ordenado E , es un subconjunto S tal que

$$x \leq s, s \in S \text{ implica } x \in S.$$

5.º El conjunto a de los elementos de E inferiores o iguales al elemento a suele llamarse *sección inicial* de a . Es, evidentemente, una parte hereditaria de E .

Diagrama y grafo de un conjunto ordenado. — Puede ser cómodo representar un conjunto ordenado mediante una figura. Cada elemento a será representado por un punto del plano, el cual se une por un trazo continuo, orientado con una flecha, a aquellos elementos b tales que $a \leq b$.

El conjunto E de los puntos y orientaciones, o *diagrama* del conjunto, con la aplicación de E en $\mathcal{P}(E)$ que asocia cada elemento a de E con el conjunto A de elementos x de E a los que se puede pasar desde a siguiendo sin interrupción la dirección de las flechas, constituye lo que se llama el *grafo* del conjunto considerado.

Ejemplos. — 1.º Si A es un conjunto cualquiera, el conjunto de sus partes o subconjuntos, $E = \mathcal{P}(A)$ está ordenado con la relación de inclusión de conjuntos. En este caso, la relación de orden se denota generalmente por $\subseteq$.

2.º Un mismo conjunto puede ser ordenado de diversas maneras. Sea $E = \{1, 2, \dots, n, \dots\}$ el conjunto de los números naturales. Se le puede ordenar:

a) de la manera habitual ($p \leq q \Leftrightarrow \exists r \in E$ tal que $p + r = q$) y entonces E es una cadena;

b) por $p \leq q \Leftrightarrow \exists r \in E$ tal que $pr = q$. Entonces no tenemos cadena;

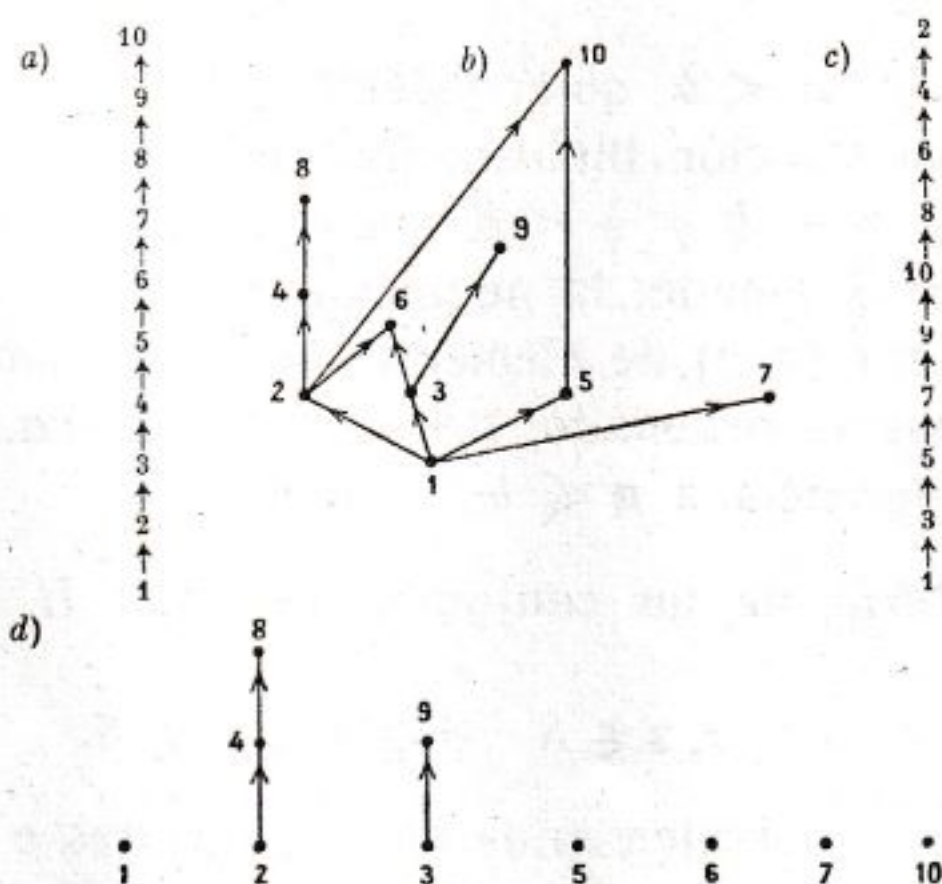
c) $2p + 1 \leq 2q \quad \forall p$ y $\forall q$; $2p + 1 \leq 2s + 1 \Leftrightarrow p \leq s$ (en el orden a); $2p \leq 2s \Leftrightarrow s \leq p$ (en el orden a); se tiene aquí la cadena

$$1, 3, 5, \dots, 2n + 1, \dots, 2n, \dots, 4, 2$$

d) $a < b \Leftrightarrow \exists p$ primo tal que $a = p^s, b = p^t, s < t$.

Se podrían indicar así muy variadas relaciones de orden en el conjunto de los números naturales.

Tracemos los diagramas del conjunto de números 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ordenado por las restricciones de las relaciones precedentes.



3.º Si E y F son dos conjuntos ordenados, también $E \times F$ se puede ordenar, poniendo:

$$(e, f) \leq (e', f') \Leftrightarrow e \leq e' \quad \text{y} \quad f \leq f'$$

relación que es reflexiva, transitiva y antisimétrica; estas propiedades resultan inmediatamente de las relaciones de orden de E y F . Señalemos que la propiedad en E y F de ser totalmente ordenados, no se conserva en $E \times F$.

4.º El conjunto de funciones reales de una variable real definidas, por ejemplo, sobre $[0, 1]$ está ordenado por

$$f \leq g \Leftrightarrow f(x) \leq g(x) \quad \forall x \in [0, 1]$$

§ 2. Elementos notables eventuales en un conjunto ordenado E

En un conjunto ordenado E , se llama:

elemento nulo o elemento inferior a un elemento 0 tal, que sea $0 \leq x$, para $\forall x \in E$; un elemento así es necesariamente único, puesto que $0 \leq 0^*$ y $0^* \leq 0$ implican $0 = 0^*$;

elemento universal o elemento superior, a un elemento u tal que se tenga $x \leq u$, para $\forall x \in E$. Este elemento es también necesariamente único;

punto o átomo a todo elemento p de E diferente de 0 y tal, que no exista elemento x de E comprendido estrictamente entre 0 y p : $0 \leq x \leq p$ implica $x = 0$ ó $x = p$.

Observación. — De modo general, en un conjunto ordenado E , se dice que b cubre a a (o que a está cubierto por b), si $a < b$ y si no existe elemento c de E comprendido estrictamente entre a y b . Un punto es, pues, un elemento que cubre a 0 .

Para un subconjunto A de E , que eventualmente puede coincidir con E , se definen también los elementos siguientes, que pueden existir o no:

elemento máximo de A : $m^* \in A$ tal que $x \leq m^*$, $\forall x \in A$;
 m^* es pues el elemento universal de A considerado como conjunto ordenado por la restricción a A del orden de E ;

elemento mínimo de A : $\mu^* \in A$ tal que $\mu^* \leq x$, $\forall x \in A$;
 μ^* es pues el elemento nulo de A .

Se llama *elemento maximal* de A un elemento m de A tal, que no existe elemento de A que le sea estrictamente superior:

$$\nexists x \in A, m < x \quad \text{o también,} \quad m \nless x, \forall x \in A$$

Un elemento así, si existe, no es necesariamente único; por ejemplo en

$\mathcal{I}(E) - \{E\}$ el elemento $E - \{a\}, (\forall a \in E)$ es maximal; y, más generalmente, en todo conjunto E que admite un elemento universal u , los elementos cubiertos por u son los elementos maximales de $E - \{u\}$.

Se llama *elemento minimal* de A un elemento μ de A tal, que no existe elemento de A que le sea estrictamente inferior.

Un elemento minimal, si existe, no es necesariamente único; por ejemplo, en $\mathcal{I}(E) - \emptyset$ todos los puntos de $\mathcal{I}(E)$ son elementos minimales; y, de modo general, si E tiene un elemento nulo, los puntos de E son los elementos minimales de $E - \{0\}$. En el conjunto de los números naturales mayores o iguales a 2 ordenado por el procedimiento $b)$, todos los números primos son elementos minimales.

Observación. — Cuando un conjunto tiene elemento máximo, este elemento es también maximal, y no existe ningún otro elemento maximal. Análogamente, el elemento mínimo es elemento minimal único.

Los elementos que vamos a introducir ahora pueden no pertenecer a A .

Se llama *elemento mayorante* de A un elemento s de E tal que $x \leq s, \forall x \in A$. Si s es un mayorante de A , todo elemento s' de E tal que $s \leq s'$ es también un mayorante de A .

Si A posee elemento máximo, este elemento es un mayorante y es el menor de los mayorantes de A . Inversamente, si A admite un mayorante que le pertenece, este elemento es elemento máximo de A , y es el menor mayorante de A .

Se llama *elemento minorante* de A un elemento t de E tal que sea $t \leq x, \forall x \in A$. Si $t' \leq t$, t' es también un minorante de A . Si A admite un elemento mínimo, es un minorante, y es el mayor de los minorantes de A .

Un subconjunto A del conjunto ordenado E es *acotado*, si admite al menos un mayorante y al menos un minorante; es *mayorado* si admite al menos un mayorante; es *minorado* si admite al menos un minorante.

Un conjunto ordenado E tal, que todo subconjunto de dos elementos esté mayorado, se dice *filtrante superiormente*.

Resulta fácilmente que:

Todo subconjunto finito de un conjunto filtrante superiormente es mayorado.

Se tiene también:

En un conjunto filtrante superiormente E , un elemento maximal es elemento máximo, y por consiguiente es único.

En efecto, si m fuera maximal sin ser máximo, existiría al menos un elemento a de E que no sería comparable con m . Pero por ser el conjunto filtrante superiormente, existirá un mayorante común a a y m , necesariamente distinto de m , y m no será por ello maximal.

Se definen de manera análoga los *conjuntos filtrantes inferiormente*: Para todo par a, b existe un minorante común:

$$\forall a \text{ y } b \in E, \quad \exists c \in E, c \leq a, \text{ y } c \leq b.$$

Conjunto filtrante es un conjunto a la vez filtrante superiormente y filtrante inferiormente.

Vamos a estudiar casos particulares importantes de conjuntos filtrantes o filtrantes por un lado.

§ 3. Semirretículos

Un *sup-semirretículo* es un conjunto ordenado en el que dos elementos cualesquiera a y b , admiten siempre un *mayorante mínimo*, que llamaremos *supremo* o *unión* de a y b , e indicaremos por la notación $\sup(a, b)$ o $a \vee b$.

Ejemplos. — 1.º Toda cadena, en particular la de los enteros ordenados de mayor a menor en el orden habitual, es un sup-semirretículo:

$$\sup(p, q) = q \quad \text{si} \quad p \leq q.$$

2.º El conjunto de los enteros positivos ordenados por la relación de divisibilidad explicada en 2b), es un sup-semirretículo; ahora $\sup(p, q)$ es el mínimo común múltiplo de p y q .

3.º En $\mathcal{I}(E)$ ordenado por la inclusión de conjuntos, se tiene $\sup(A, B) = A \cup B$, es decir, la unión en el sentido de la teoría de conjuntos.

Observación. — $\mathcal{I}(E) - \{E\}$ no es sup-semirretículo; pues, si a y b son diferentes,

$$(E - \{a\}) \cup (E - \{b\})$$

no existe en $\mathcal{I}(E) - \{E\}$, si $a \in E$ y $b \in E$ son elementos diferentes.

Proposición. — En un sup-semirretículo todo subconjunto finito admite un mayorante mínimo, al que también llamamos supremo, o unión, del subconjunto.

Se demuestra inmediatamente por recurrencia. Sea cierto para subconjuntos de menos de $n \geq 2$ elementos: ponemos $b = \sup(a_1, \dots, a_{n-1})$, los elementos b y a_n tienen un mayorante mínimo c que entonces mayor a $a_1, \dots, a_{n-1}, a_n$; sea ahora m otro mayorante de $a_1, \dots, a_n$. En particular, m mayor a $a_1, \dots, a_{n-1}$, luego a b y a a_n luego a c , de donde c es mayorante mínimo de $a_1, \dots, a_n$.

Generalización. — Un *sup-semirretículo completo* es un sup-semirretículo en el cual todo subconjunto S admite un mayorante mínimo (llamado como antes, *supremo* o *unión* de S).

En particular, un sup-semirretículo completo admite un elemento universal.

Por ejemplo, en $\mathcal{F}(E)$ una familia cualquiera de elementos

$$A_i (A_i \subseteq E, \forall i \in I)$$

tiene como supremo su unión en el sentido de la teoría de conjuntos: $\sup A_i = \{x; x \in E, \exists i \in I, x \in A_i\} = \bigcup_{i \in I} A_i$, por lo tanto $\mathcal{F}(E)$ es un sup-semirretículo completo.

En cambio el conjunto de naturales con su orden habitual no tiene mayorante mínimo. Es un sup-semirretículo no completo.

De manera análoga se define un *inf-semirretículo*:

Un inf-semirretículo es un conjunto ordenado en el cual dos elementos a y b cualesquiera admiten un minorante máximo que llamaremos infimo de a y b , al que designaremos por $\inf(a, b)$ ó $a \wedge b$.

Por ejemplo en toda cadena, en particular en el conjunto de números naturales ordenados por el procedimiento habitual, se tiene:

$$\inf(p, q) = p \text{ si } p \leq q.$$

Análogamente, el conjunto de números naturales ordenado por el procedimiento 2 b) es un inf-semirretículo, con $\inf(p, q) = \text{m.c.d.}(p, q)$.

$\mathcal{F}(E)$ es igualmente un inf-semirretículo, y se tiene $\inf(A, B) = A \cap B$. Pero es necesario observar que $\mathcal{F}(E) - \emptyset$ no es un inf-semirretículo puesto que el límite inferior de dos puntos distintos no pertenece a $\mathcal{F}(E) - \emptyset$. Análogamente el conjunto de números naturales mayores o iguales que 2 ordenado por el procedimiento 2 b) no es un inf-semirretículo, puesto que el m.c.d. de dos números primos no es un entero mayor o igual que 2.

En un inf-semirretículo todo subconjunto finito admite un minorante máximo; se llama *inf-semirretículo completo* un inf-semirretículo en el cual *todo* subconjunto admite un minorante máximo, o infimo. En particular, un inf-semirretículo completo admite elemento mínimo.

Por ejemplo $\mathcal{F}(E)$ es un inf-semirretículo completo. Por el contrario la cadena de números reales $1/n$ para $n = 1, 2, \dots$, con el $\leq$ habitual, no es un inf-semirretículo completo.

§ 4. Retículos

Un retículo es un conjunto ordenado que es a la vez inf- y sup-semirretículo. Dicho de otra manera, un retículo es un conjunto ordenado en el cual todo par de elementos admite un mayorante mínimo y un minorante máximo, es decir, un supremo y un infimo.

De lo visto en el párrafo anterior, resulta que todo subconjunto finito de un retículo es acotado.

Si E y F son retículos, el conjunto producto $E \times F$, ordenado como se ha visto en § 1, es también un retículo.

Observemos que un subconjunto $\mathcal{A}$ de un retículo o de un semirretículo $\mathcal{G}$ ordenado por la restricción a $\mathcal{A}$ de la relación de orden de $\mathcal{G}$ no es necesariamente un retículo o un semirretículo; por ejemplo $\mathcal{A} = \mathcal{P}(E) - \{\emptyset, E\}$ no es ni un retículo ni un semirretículo; pero hay más, un subconjunto $\mathcal{A}$ de un retículo o de un semirretículo $\mathcal{G}$ ordenado por la restricción a $\mathcal{A}$ de la relación de orden de $\mathcal{G}$ puede ser un retículo sin que, para un par de elemento de $\mathcal{A}$, el supremo e ínfimo sean los mismos en $\mathcal{A}$ y en $\mathcal{G}$. Pero sí se tiene, naturalmente:

$$\inf_{\mathcal{A}}(a, a') \leq \inf_{\mathcal{G}}(a, a') \leq \sup_{\mathcal{G}}(a, a') \leq \sup_{\mathcal{A}}(a, a'), \quad \forall a \text{ y } a' \in \mathcal{A}.$$

Si $\inf_{\mathcal{A}}(a, a') = \inf_{\mathcal{G}}(a, a')$ y $\sup_{\mathcal{G}}(a, a') = \sup_{\mathcal{A}}(a, a')$ para todo par de elementos (a, a') de $\mathcal{A}$, se dice que $\mathcal{A}$ es un *subretículo* de $\mathcal{G}$.

Diremos que dos conjuntos ordenados E y E^* son *isomorfos*, si existe una aplicación biyectiva α de E sobre E^* tal que cada una de las relaciones $a \leq b$, $\alpha(a) \leq \alpha(b)$ implica la otra.

Lema. — Si E y E^* son dos conjuntos ordenados isomorfos, y si en E por ejemplo, un conjunto A de elementos a , admite supremo s , o ínfimo i , las imágenes $\alpha(s)$, $\alpha(i)$, son también respectivamente supremo e ínfimo del conjunto $\alpha(A)$ de las imágenes de los elementos de A , en E^* .

En efecto, $i \leq a \leq s$ para todo $a \in A \rightarrow \alpha(i) \leq \alpha(a) \leq \alpha(s)$, luego $\alpha(i)$ es un minorante y $\alpha(s)$ un mayorante para $\alpha(A)$. Y si se tiene $x^* \leq \alpha(a) \leq y^*$ para $\forall a \in A$, se deduce de ello, poniendo $x = \alpha^{-1}(x^*)$, $y = \alpha^{-1}(y^*)$, que $x \leq a \leq y$, $\forall a \in A$, luego $x \leq i$, $s \leq y$ de donde $x^* \leq \alpha(i)$, $\alpha(s) \leq y^*$.

Corolario. — Dos retículos isomorfos como conjuntos ordenados, lo son como retículos (es decir, tomando sup e inf como leyes de composición).

Definición. — Un retículo es completo si es a la vez inf y sup-semirretículo completo.

Así, $\mathcal{P}(E)$ es un retículo completo.

Si E y F son retículos completos, el retículo $E \times F$ también lo es.

Consideremos finalmente el conjunto de funciones reales definidas ≥ 0 y acotadas superiormente sobre el intervalo cerrado $[0, 1]$, ordenado como se ha visto en § 1. Este conjunto, que es un retículo, es un inf-semirretículo completo. Si se supone que todas las funciones son acotadas superiormente en su conjunto por un número fijo, entonces constituyen un retículo completo.

Teorema 1. — Todo semirretículo completo $\mathcal{A}$ que tiene un elemento nulo 0 y un elemento universal u es un retículo completo $\mathcal{G}$.

Para fijar ideas, tomemos un inf-semirretículo completo, lo que implica la existencia del elemento nulo 0, y tomemos un subconjunto cualquiera S de $\mathcal{A}$.

El conjunto $\mathcal{M}$ de los mayorantes de S en $\mathcal{A}$, no es vacío puesto que u existe y $u \in \mathcal{M}$.

$\mathcal{M}$ es un subconjunto de $\mathcal{A}$, luego admite un minorante máximo μ ; pero, si $s \in S$, se tiene $s \leq m \ \forall m \in \mathcal{M}$. Luego s es un minorante de $\mathcal{M}$, por lo que $s \leq \mu$ y esto para todo elemento s de S . Por consiguiente μ es mayorante de S : $\mu \in \mathcal{M}$ y es el elemento mínimo de $\mathcal{M}$.

Según la definición dada en el capítulo I, una *familia de Moore* $\mathcal{F}$ de partes de un conjunto E es un inf-semirretículo completo con elemento universal E . $\mathcal{F}$ es por consiguiente, según el teorema 1 un retículo completo en el cual el mayorante mínimo de un subconjunto S de $\mathcal{F}$, $\sup_{S \in S} S$, está definido de la manera siguiente. Sea $\mathcal{M}$ el subconjunto de $\mathcal{F}$ formado por las partes M que mayoran a S :

$$\mathcal{M} = \{ M ; M \in \mathcal{F}, S \subseteq M \ \forall S \in S \}.$$

Tenemos

$$(1) \quad \sup_{S \in S} S = \inf_{M \in \mathcal{M}} M = \bigcap_{M \in \mathcal{M}} M.$$

Podemos inmediatamente generalizar lo que precede reemplazando el retículo $\mathcal{P}(E)$ de las partes de un conjunto E por un retículo completo cualquiera $\mathcal{G}$, en el cual continuaremos designando los elementos por letras mayúsculas y en el cual la relación de orden, el supremo y el ínfimo, serán indicados respectivamente con $\leq$, $\vee$ y $\wedge$. Una parte $\mathcal{F}$ de $\mathcal{G}$ se llama *familia de Moore* si verifica las dos condiciones siguientes:

- I. El elemento máximo U de $\mathcal{G}$ pertenece a $\mathcal{F}$.
- II. Para toda parte no vacía S de $\mathcal{F}$, se tiene

$$\bigwedge_{S \in S} S \in \mathcal{F}.$$

Según II, $\mathcal{F}$ es un inf-semirretículo completo que tiene elemento máximo según I, luego en virtud del teorema 1, $\mathcal{F}$ es un retículo completo. El supremo, en $\mathcal{F}$, de toda parte no vacía S , $\sup S$, se obtiene como más arriba. Designando con $\mathcal{M}$ el conjunto de elementos M de $\mathcal{F}$ que mayoran a S :

$$\mathcal{M} = \{ M ; M \in \mathcal{F}, S \leq M \ \forall S \in S \},$$

tenemos

$$(1) \quad \sup_{S \in S} S = \bigwedge_{M \in \mathcal{M}} M.$$

A todo elemento X de $\mathcal{C}$ podemos asociarle el elemento mínimo $\bar{X}$ de $\mathcal{F}$ que contiene a X : designando por S el conjunto de elementos S de $\mathcal{F}$ superiores o iguales a X , tenemos

$$\bar{X} = \bigwedge_{S \in \mathcal{S}} S \quad (\in \mathcal{F}).$$

Es claro que, para un elemento F de $\mathcal{F}$ se tiene $\bar{F} = F$ y que la aplicación $X \rightarrow \bar{X}$ de $\mathcal{C}$ en $\mathcal{F}$ es extensiva ($X \leq \bar{X}$), isótoma ($X \leq Y$ implica $\bar{X} \leq \bar{Y}$) e idempotente ($\bar{\bar{X}} = \bar{X}$ puesto que $\bar{X} \in \mathcal{F}$). Esta aplicación será llamada de ahora en adelante *clausura de Moore* asociada a la familia $\mathcal{F}$.

Consideremos entonces un subconjunto cualquiera $\mathcal{X}$ de $\mathcal{C}$. Tenemos la fórmula

$$(2) \quad \overline{\bigvee_{X \in \mathcal{X}} X} = \bigvee_{X \in \mathcal{X}} \bar{X} = \sup_{X \in \mathcal{X}} \bar{X}$$

que generaliza la fórmula establecida en el capítulo I (§ 5) para el caso $\mathcal{C} = \mathcal{P}(E)$, que escribimos

$$\overline{\bigcup_{X \in \mathcal{X}} X} = \bigcup_{X \in \mathcal{X}} \bar{X} = \sup_{X \in \mathcal{X}} \bar{X}.$$

De $X \leq \bar{X}$, obtenemos $\bigvee_{X \in \mathcal{X}} X \leq \bigvee_{X \in \mathcal{X}} \bar{X}$, luego $\overline{\bigvee_{X \in \mathcal{X}} X} \leq \overline{\bigvee_{X \in \mathcal{X}} \bar{X}}$.

Por otra parte, $\bar{X} \leq \sup_{X \in \mathcal{X}} \bar{X} (\in \mathcal{F})$ implica $\bigvee_{X \in \mathcal{X}} \bar{X} \leq \sup_{X \in \mathcal{X}} \bar{X}$, de donde

$$\overline{\bigvee_{X \in \mathcal{X}} \bar{X}} \leq \sup_{X \in \mathcal{X}} \bar{X}.$$

Finalmente, $X \leq \bigvee_{X \in \mathcal{X}} X$ implica $\bar{X} \leq \overline{\bigvee_{X \in \mathcal{X}} X} (\in \mathcal{F})$ luego $\sup_{X \in \mathcal{X}} \bar{X} \leq \overline{\bigvee_{X \in \mathcal{X}} X}$.

La doble igualdad (2) resulta de las tres inclusiones que acabamos de establecer.

En particular, para un subconjunto S de $\mathcal{F}$, tenemos:

$$(3) \quad \sup_{S \in \mathcal{S}} S = \overline{\bigvee_{S \in \mathcal{S}} S} \quad (S \subseteq \mathcal{F}).$$

Resumiendo, podemos enunciar:

Teorema 2. — *Una familia de Moore $\mathcal{F}$ en un retículo completo $\mathcal{C}$ es también un retículo completo, cuyo infimo coincide con el $\wedge$ de $\mathcal{C}$, mientras que el supremo viene dado por las fórmulas (1) y (3). Se tiene además, para un subconjunto $\mathcal{X}$ cualquiera de $\mathcal{C}$, la fórmula (2).*

Corolario. — *La equivalencia de clausura $\mathcal{R}$ definida en $\mathcal{C}$ a partir de $\mathcal{F}$ por*

$$X \equiv X_1(\mathcal{R}) \quad \text{si} \quad \bar{X} = \bar{X}_1$$

es compatible con $\vee$ según la fórmula (2).

Ejemplos. — 1. En un *semigrupo* (multiplicativo) D , las *partes estables* S forman una familia de Moore, y por lo tanto un retículo completo, en el cual

$$\inf(S_1, S_2) = S_1 \cap S_2$$

mientras que

$$\sup(S_1, S_2) = \overline{S_1 \cup S_2}$$

es la parte estable engendrada por $S_1 \cup S_2$, es decir el conjunto de los productos (finitos) formados con elementos tomados en S_1 y S_2 .

2. En un *grupo* G , los *subgrupos* H forman una familia de Moore, luego también un retículo completo $\mathcal{H}$, en el cual

$$\inf(H_1, H_2) = H_1 \cap H_2$$

mientras que

$$\sup(H_1, H_2) = \overline{H_1 \cup H_2}$$

es el subgrupo engendrado por $H_1 \cup H_2$, es decir su reunión completa (Cap. III, § 1), conjunto de los productos finitos formados con elementos tomados en H_1 y H_2 .

Así mismo, el conjunto de los *subgrupos distinguidos* del grupo G es una familia de Moore, luego es un retículo completo $\mathcal{D}$. Ahora bien, la reunión completa de una familia de subgrupos distinguidos, que es también su producto, es un subgrupo distinguido: $\mathcal{D}$ es pues un *subretículo* del retículo $\mathcal{H}$ de todos los subgrupos. Volveremos (§ 8) a tratar del retículo de los subgrupos distinguidos de un grupo G .

En un *anillo* A , designamos por $\mathcal{S}$ la familia de los subgrupos aditivos, por $\mathcal{I}_i$, $\mathcal{I}_a$, $\mathcal{I}$ las familias de los *ideales a la izquierda*, de los *ideales a la derecha* y de los *ideales biláteros* de A ; $\mathcal{S}$, $\mathcal{I}_i$, $\mathcal{I}_a$, $\mathcal{I}$ son familias de Moore y, por consi-

guiente, retículos completos. En $\mathcal{S}$, el supremo coincide con la suma; ocurre lo mismo en los retículos $\mathcal{I}_i$, $\mathcal{I}_a$, $\mathcal{I}_f$ puesto que un grupo aditivo suma de ideales es un ideal (Cap. IV, § 7). De ello resulta que $\mathcal{I}_i$ y $\mathcal{I}_a$ son *subretículos* de $\mathcal{S}$, y que $\mathcal{I}$ es un *subretículo* de $\mathcal{I}_i$ y de $\mathcal{I}_a$. Más adelante (§ 8 y § 10) insistiremos sobre los retículos de ideales.

3. Dado un conjunto E , consideremos los subconjuntos $\mathcal{F}$ de $\mathcal{P}(E)$ estables para la intersección $\cap$ y licitos para la unión $\cup$:

- 1) $F_1 \in \mathcal{F}, F_2 \in \mathcal{F} \Rightarrow F_1 \cap F_2 \in \mathcal{F}$;
- 2*) $F_1 \in \mathcal{F}, X \in \mathcal{P}(E) \Rightarrow F_1 \cup X \in \mathcal{F}$.

El conjunto de estas partes $\mathcal{F}$ de $\mathcal{P}(E)$ es una familia de Moore, luego es un retículo.

Observación. — Sea $Y \in \mathcal{P}(E)$ con $Y \supset F_1 \in \mathcal{F}$, se tiene entonces

$Y \cup F_1 = Y$; ahora bien $F_1 \in \mathcal{F} \Rightarrow F_1 \cup Y \in \mathcal{F}$ según 2), y por consiguiente $Y \cup F_1 = Y$ implica

$$2) F_1 \in \mathcal{F}, Y \supset F_1 \Rightarrow Y \in \mathcal{F}.$$

Recíprocamente si una familia de partes de E verifica 1) y 2), resulta de ello, si $F_1 \in \mathcal{F}$ y $X \in \mathcal{P}(E)$, que $F_1 \cup X$ contiene a F_1 perteneciente a $\mathcal{F}$, es decir 2*).

Luego el sistema de condiciones 1) y 2) es equivalente al sistema de las condiciones 1) y 2*).

En topología, se llama precisamente *filtro* una familia $\mathcal{F}$ de partes del conjunto E que verifica estas condiciones:

- 1) $F_1 \in \mathcal{F}, F_2 \in \mathcal{F} \Rightarrow F_1 \cap F_2 \in \mathcal{F}$;
- 2) $F \in \mathcal{F}, X \supseteq F \Rightarrow X \in \mathcal{F}$;
- 3) $\emptyset \notin \mathcal{F}$.

La 3) expresa que el filtro considerado no es $\mathcal{P}(E)$, pues $\mathcal{P}(E)$ contiene a $\emptyset$ e inversamente, si una familia $\mathcal{F}$ que verifica 1) y 2) contiene a $\emptyset$, en virtud de 2) contiene toda parte X de E . Los filtros son por consiguiente los elementos de la precedente familia de Moore, distintos del máximo $\mathcal{P}(E)$, que se llama filtro impropio.

Podemos enunciar:

Teorema 3. — Los filtros de E constituyen con $\mathcal{P}(E)$ una familia de Moore, que llamaremos la familia de Moore de los filtros de E .

Consideremos entonces dos filtros $\mathcal{F}$ y $\mathcal{F}^*$ de E ; $\inf(\mathcal{F}, \mathcal{F}^*)$ es la intersección $\mathcal{F}'$ de estas dos familias en $\mathcal{P}(E)$, es decir el conjunto

$$\mathcal{F}' = \{ F' ; F' \subseteq E, F' \in \mathcal{F}, F' \in \mathcal{F}^* \}.$$

Se tiene $\mathcal{F}' = \Phi$ donde

$$\Phi = \{ F \cup F^* ; F \in \mathcal{F}, F^* \in \mathcal{F}^* \}$$

En efecto $F \cup F^* \supseteq F$ implica $F \cup F^* \in \mathcal{F}$; así mismo $F \cup F^* \supseteq F^*$ implica $F \cup F^* \in \mathcal{F}^*$, de donde $F \cup F^* \in \mathcal{F}'$ y por consiguiente $\Phi \subseteq \mathcal{F}'$.

Recíprocamente, sea $F' \in \mathcal{F}'$, $F' = F' \cup F'$ es pues un elemento de Φ y tenemos $\mathcal{F}' \subseteq \Phi$, de donde sigue la igualdad. Por consiguiente podemos escribir

$$\inf(\mathcal{F}, \mathcal{F}^*) = \{ F \cup F^* ; F \in \mathcal{F}, F^* \in \mathcal{F}^* \}$$

En cuanto a $\sup(\mathcal{F}, \mathcal{F}^*)$ es el filtro engendrado por la parte de $\mathcal{I}(E)$ que es la unión en el sentido de la teoría de conjuntos de las partes $\mathcal{F}$ y $\mathcal{F}^*$.

Como parte estable para la intersección, este filtro contiene el conjunto $\mathcal{J}$ de las intersecciones $F \cap F^*$ donde $F \in \mathcal{F}$, $F^* \in \mathcal{F}^*$. Pero este conjunto $\mathcal{J}$ es lícito para la reunión puesto que

$$(F \cap F^*) \cup X = (F \cup X) \cap (F^* \cup X)$$

y

$$F \cup X \in \mathcal{F}, \quad F^* \cup X \in \mathcal{F}^*, \quad \forall X \in \mathcal{I}(E).$$

$\mathcal{J}$ es, pues, el filtro buscado:

$$\sup(\mathcal{F}, \mathcal{F}^*) = \{ F \cap F^* ; F \in \mathcal{F}, F^* \in \mathcal{F}^* \}$$

Puesto que hemos tratado con retículos completos, se tiene también para cualquier familia de filtros,

$$\begin{aligned} \sup_{i \in I} (\mathcal{F}_i) &= \{ \bigcap F_i ; F_i \in \mathcal{F}_i, i \in I \} \\ \inf_{i \in I} (\mathcal{F}_i) &= \{ \bigcup F_i ; F_i \in \mathcal{F}_i, i \in I \} \end{aligned}$$

Naturalmente puede ocurrir que $\sup(\mathcal{F}, \mathcal{F}^*)$ no sea un filtro, sino el filtro impropio $\mathcal{I}(E)$; será así si existen $F \in \mathcal{F}$ y $F^* \in \mathcal{F}^*$ tales que $F \cap F^* = \emptyset$ y sólo en este caso.

De modo general, si $\mathcal{M}$ es una familia de partes no vacías de E , el filtro $\mathcal{F}$ engendrado por $\mathcal{M}$ contiene como elementos todas las intersecciones finitas de partes de $\mathcal{M}$, luego contiene la familia $\cap$ -estable engendada por $\mathcal{M}$.

En virtud de la condición 2), $\mathcal{F}$ es el conjunto de las partes de E que contienen una tal intersección finita. Luego el sistema de generadores $\mathcal{M}$ engendra un filtro $\neq \mathcal{I}(E)$ si, y sólo si, ninguna intersección finita de elementos de $\mathcal{M}$ es vacía.

Entre los sistemas de generadores $\mathcal{M}$ que engendran el mismo filtro $\mathcal{F}$ (elementos de la clase de $\mathcal{F}$ en la equivalencia de clausura de Moore en $\mathcal{I}(E)$), se llama *base de filtro* los que tienen la propiedad siguiente:

Existe un elemento de $\mathcal{M}$ contenido en toda intersección finita de elementos de $\mathcal{M}$.

Naturalmente una base de filtro no engendra nunca el filtro impropio $\mathcal{I}(E)$, y de aquí su interés.

Entre los sistemas de generadores de un filtro, existe siempre al menos una base de filtro: el mismo filtro.

Pero, por ejemplo, $\mathcal{F} \cup \mathcal{F}^*$ no es en general una base de filtro para $\sup(\mathcal{F}, \mathcal{F}^*)$.

Se obtienen bases de filtro de la manera siguiente. Sea $\mathcal{F}'$ un filtro en un conjunto E' ; toda aplicación α de E' en E , aplica $\mathcal{F}'$ sobre una base de filtro en E . En efecto:

$$\mathcal{M} = \{ \alpha(F') ; F' \in \mathcal{F}' \}$$

es un subconjunto de $\mathcal{I}(E)$ que engendra un filtro de E y si $F_1 \in \mathcal{M}$, $F_2 \in \mathcal{M}$, existe $F'_1 \in \mathcal{F}'$ y $F'_2 \in \mathcal{F}'$ tales que

$$\alpha(F'_1) = F_1, \quad \alpha(F'_2) = F_2,$$

de donde

$$\alpha(F'_1 \cap F'_2) \subseteq \alpha(F'_1) \cap \alpha(F'_2) = F_1 \cap F_2$$

y

$$\alpha(F'_1 \cap F'_2) \in \mathcal{M}$$

está contenido en $F_1 \cap F_2$.

Luego la imagen, en un conjunto E , de un filtro de E' por una aplicación α de E' en E , es una base de filtro.

Se tiene además $F_1 \cap F_2 \in \mathcal{M}$; en efecto,

$$F_i'^* = \alpha^{-1}[\alpha(F_i')] \supseteq F_i', \text{ luego } F_i'^* \in \mathcal{F}' \ (i = 1, 2);$$

ahora bien

$$F'_1 \cap F'_2 \in \mathcal{F}'$$

y por consiguiente:

$$F_1 \cap F_2 = \alpha(F'_1 \cap F'_2) \in \mathcal{M}.$$

Si α aplica E' sobre E , la base de filtro $\mathcal{M} = \alpha(\mathcal{F}')$ es un filtro. Sea en efecto $X \supseteq F_1$ ($X \subseteq E$, $F_1 \in \mathcal{M}$), la aplicación α es exhaustiva, luego $\alpha^{-1}(X)$ existe

y verifica

$$\alpha^{-1}(X) \supseteq \alpha^{-1}(F_1),$$

de donde

$$\alpha^{-1}(X) \in \mathcal{F}' \quad \text{y} \quad X = \alpha[\alpha^{-1}(X)] \in \mathcal{M}.$$

Ejemplos de filtros. — 1. El conjunto de las partes de E que contienen una parte dada $A \neq \emptyset$ es un filtro llamado *filtro principal de A* , $\mathcal{F}(A)$. En efecto,

$$1^\circ \quad A_1 \supseteq A \text{ y } A_2 \supseteq A \quad \text{implican} \quad A_1 \cap A_2 \supseteq A,$$

luego

$$A_1 \cap A_2 \in \mathcal{F}(A).$$

2° $X \in \mathcal{P}(E)$ y $A_1 \in \mathcal{F}(A)$, es decir $A_1 \supseteq A$, implican $A_1 \cup X \supseteq A$,
luego $A_1 \cup X \in \mathcal{F}(A)$

$$3^\circ \quad \emptyset \notin \mathcal{F}(A).$$

2. El conjunto de los complementarios de los subconjuntos finitos del conjunto E supuesto infinito es un filtro. En efecto:

$$1^\circ \quad \complement_E(A_1 \cap A_2) = \complement_E A_1 \cup \complement_E A_2 \text{ es una parte finita de } E.$$

$$2^\circ \quad X \in \mathcal{P}(E) \text{ y } \complement_E A \text{ finito implican}$$

$$\complement_E(X \cup A) = \complement_E X \cap \complement_E A \subseteq \complement_E A,$$

luego $\complement_E(X \cup A)$ es finito.

$$3^\circ \quad \complement_E \emptyset = E \text{ es infinito por hipótesis.}$$

3. Así mismo, el conjunto de los complementarios de las partes numerables de un conjunto E no numerable es un filtro.

Indiquemos todavía una proposición importante: *el teorema de Mac Neille*.

Sea E un conjunto ordenado; consideremos la aplicación α de $\mathcal{P}(E)$ en $\mathcal{P}(E)$ que asocia a cada parte A de E el conjunto A^* de los minorantes del conjunto M_A de los mayorantes de A :

$$\begin{aligned} M_A &= \{ m; a \leq m \quad \forall a \in A \}, \\ A^* &= \{ x; x \leq m \quad \forall m \in M_A \}, \\ (a) \quad &A \rightarrow A^*. \end{aligned}$$

Si $A = \emptyset$, se tiene $M_A = E$ y, si E posee un elemento mínimo z , $A^* = \{ z \}$; en caso contrario, $A^* = \emptyset$. Si el conjunto M_A de los mayorantes de A es vacío,

A^* no es otro que E .

La aplicación α así definida posee las propiedades siguientes:

1.º Se tiene por construcción $A \subseteq A^* : \alpha$ es *extensiva*.

2.º Sea $A \subseteq B$; el conjunto M_B de los mayorantes de B está contenido en el conjunto M_A de los mayorantes de A , de donde $A^* \subseteq B^* : \alpha$ es *isótona*.

3.º Puesto que tenemos $A \subseteq A^*$, todo mayorante m^* de A^* es un mayorante de A ; pero inversamente, todo mayorante m de A mayor a A^* , por definición: luego $M_A = M_{A^*}$ y por consiguiente $A^* = A^{**} : \alpha$ es *idempotente*.

Por tener esas tres propiedades, α es una *clausura de Moore*; los cerrados $\alpha(A) = A^*$ constituyen una *familia de Moore*, y por ende un *retículo completo* $\mathcal{C}$ [subconjunto de $\mathcal{P}(E)$]. La relación de orden $\mathcal{C}$ es la inclusión de las partes y el inf, en $\mathcal{C}$, coincide con la intersección conjuntista.

Consideremos la parte $\{x\}$ con un solo elemento x de E ; su imagen $\{x\}^*$, que designaremos simplemente por x^* , es el conjunto S_x de los elementos $s \leq x$ en el orden de E : S_x es llamado *sección inicial* de x . Se indica también con el símbolo $\bar{x}$. Sea $\mathcal{S} (\subseteq \mathcal{C})$ el conjunto de los $x^* = S_x$ cuando x recorre E ; la aplicación

$$\bar{\alpha} \quad x \rightarrow x^*$$

de E sobre $\mathcal{S}$ es evidentemente biyectiva; $x \leq y$ en E implica $x^* \subseteq y^*$ en $\mathcal{S}$ y reciprocamente; los conjuntos ordenados $E, \mathcal{S}$ son *isomorfos*.

Según el teorema 2 y las fórmulas (2) y (3), el supremo, Sup, en $\mathcal{C}$, viene dado por:

$$(3') \quad \text{Sup}_{F \in \mathcal{F}} F = \left(\bigcup_{F \in \mathcal{F}} F \right)^* \quad (\mathcal{F} \subseteq \mathcal{C})$$

y se tiene para una familia cualquiera $\mathcal{X}$ de partes de E :

$$(2') \quad \text{Sup}_{X \in \mathcal{X}} X^* = \left(\bigcup_{X \in \mathcal{X}} X \right)^*.$$

Si A es un subconjunto (finito o infinito) de E tal que, en el orden de E , $\sup_{a \in A} a = h$ existe y si $x \in h^* = S_h$, x , menor o igual al elemento mínimo del conjunto M_A de los mayorantes de A , es un minorante de M_A , luego $x \in A^*$; tenemos pues $h^* \subseteq A^*$. Pero inversamente, puesto que $h \in M_A$, el conjunto A^* de los minorantes de M_A está contenido en h^* , de donde la igualdad:

$$(4) \quad A^* = h^*.$$

De ello resulta, en primer lugar, que toda igualdad de la forma $\sup A = \sup B$ en E implica $A^* = B^*$.

Por otra parte, reemplacemos A por $\bigcup_{a \in A} \{a\}$; tenemos, según (2')

$$A^* = \sup_{a \in A} a^* ;$$

la igualdad (4) se escribe entonces

$$(5) \quad \sup_{a \in A} a^* = \left(\sup_{a \in A} a \right)^*,$$

lo que expresaremos diciendo que *la inmersión de E en el retículo completo $\mathfrak{C}$ conserva el mayorante mínimo, o supremo.*

Si, finalmente, A es una parte de E con un minorante máximo, $i = \inf_{a \in A} a$ en el orden E , $i^* = S_i$ es el conjunto de los minorantes de A ; ahora bien $a^* = S_a$ es el conjunto de los minorantes de a y por consiguiente la intersección

$$\bigcap_{a \in A} a^*$$

es el conjunto de los minorantes de A , es decir i^* ; tenemos entonces

$$(6) \quad \bigcap_{a \in A} a^* = \left(\inf_{a \in A} a \right)^*$$

por lo que *el infimo también se conserva.* Podemos enunciar:

Teorema 4 (Mac Neille). — *Todo conjunto ordenado E puede sumergirse en un retículo completo $\mathfrak{C}$ de modo que el supremo y el infimo se conserven.*

Observación. — Si E es el conjunto de los números racionales con el orden habitual $\leq$ (orden total), se obtiene para $\mathfrak{C}$ un retículo completo que, salvo isomorfismos, no es otro que el conjunto de los números reales al cual se adjuntan un elemento mínimo ($-\infty$, correspondiente a $\emptyset$) y un elemento máximo ($+\infty$, correspondiente a E). El teorema de Mac Neille generaliza, pues, la definición de los números reales por el método de Dedekind.

§ 5. Definición algebraica de un semirretículo o de un retículo

En el precedente § 4 hemos introducido los retículos y los semirretículos a partir de una relación de orden.

Vamos ahora a vincular ese punto de vista conjuntista y el punto de vista algebraico, considerando un semirretículo o un retículo, como un conjunto en el cual se han definido una o dos leyes de composición interna.

En un inf-semirretículo, por ejemplo, a cada par de elementos a y b se puede asociar el elemento $\inf(a, b)$; se define así una ley de composición interna que denotaremos por un signo de operación, por ejemplo $a \wedge b$, que según su definición es, evidentemente,

I. *idempotente*: $a \wedge a = a$,

II. *conmutativa*: $a \wedge b = b \wedge a$,

III. *asociativa* puesto que: $(a \wedge b) \wedge c = a \wedge (b \wedge c) = \inf(a, b, c)$.

Inversamente, consideremos un *semigrupo* (o *monoide*) *abeliano* D en el que denotaremos con $\top$ la operación, que supondremos *idempotente*. Consideremos entonces la relación $\mathcal{R}$ definida por

$$a\mathcal{R}b \text{ si } a \top b = a;$$

en virtud de la idempotencia, es *reflexiva*: $a \top a = a$ implica $a\mathcal{R}a$; en virtud de la conmutatividad, es *antisimétrica* puesto que:

$$a\mathcal{R}b, (a \top b = a) \quad \text{y} \quad b\mathcal{R}a (b \top a = b) \quad \text{implican} \quad a \top b = a = b.$$

En fin, es *transitiva*,

$a\mathcal{R}b$ y $b\mathcal{R}c$, es decir $a \top b = a$ y $b \top c = b$ implican $a \top c = (a \top b) \top c$, de donde en virtud de la asociatividad:

$$a \top c = a \top (b \top c) = a \top b = a,$$

es decir $a\mathcal{R}c$.

$\mathcal{R}$ es, pues, una relación de orden.

Además, *el conjunto D así ordenado es un inf-semirretículo*. Se tiene en efecto $(a \top b) \mathcal{R}b$ puesto que $(a \top b) \top b = a \top b$ en virtud la asociatividad y de la idempotencia.

Lo mismo, $(a \top b) \mathcal{R}a$ puesto que $(a \top b) \top a = a \top b$ en virtud de la asociatividad, la conmutatividad y la idempotencia.

El conjunto ordenado es, pues, filtrante inferiormente.

Sea entonces μ tal que $\mu\mathcal{R}a$ y $\mu\mathcal{R}b$, es decir:

$$\mu \top a = \mu \quad \text{y} \quad \mu \top b = \mu.$$

Se deduce de ello: $\mu \top (a \top b) = \mu$, luego $\mu\mathcal{R}(a \top b)$.

Luego, $a \top b$ es el minorante máximo de a y b , y D es un *inf-semirretículo*.

Observaciones. — 1. Para una ley de composición interna los axiomas de idempotencia, conmutatividad y asociatividad, son independientes; esto se ve fácilmente sobre ejemplos.

2. Asociada también a la ley de composición interna asociativa, conmutativa e idempotente $\top$, se habría podido definir otra relación de orden, llamada *opuesta o dual*: $a\mathcal{R}'b$ si $a \top b = b$.

En un retículo se puede, también, asociar a cada par de elementos a, b los elementos $\inf(a, b)$ y $\sup(a, b)$, y, por esto, definir dos leyes de composición interna que denotaremos con los signos de operación:

$$a \wedge b = \inf(a, b)$$

$$a \vee b = \sup(a, b)$$

estas dos operaciones son, por su definición, *asociativas, conmutativas e idempotentes*.

En general, una no es distributiva respecto de la otra, pero están ligadas por la *ley de absorción*

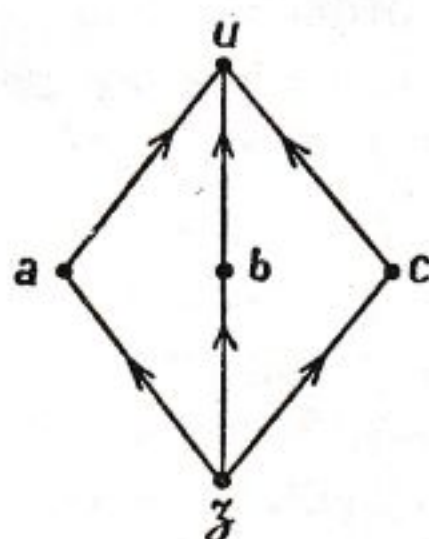
$$(IV) \quad a \wedge (a \vee b) = a, \quad a \vee (a \wedge b) = a;$$

estas igualdades resultan de que a mayor a $a \wedge b$ y es mayorado por $a \vee b$.

Se llama retículo *distributivo* un retículo en el cual cada una de las dos operaciones $\wedge, \vee$ es distributiva para la otra; veremos más adelante que estas dos distributividades no son independientes.

Ejemplos de retículos no distributivos. — 1. El conjunto ordenado de 5 elementos, cuyo diagrama es:

(M)

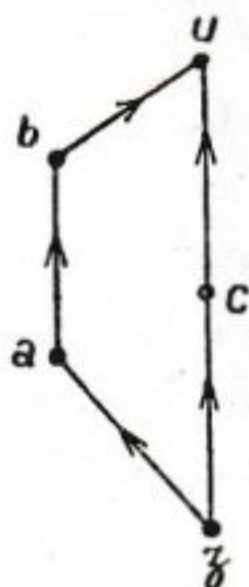


no es distributivo, ya que se tienen las igualdades

$$\begin{cases} a \vee (b \wedge c) = a \vee z = a, \\ (a \vee b) \wedge (a \vee c) = u \wedge u = u \quad \text{pues } a \neq u; \\ a \wedge (b \vee c) = a \wedge u = a, \\ (a \wedge b) \vee (a \wedge c) = z \vee z = z, \quad \text{y } a \neq z. \end{cases}$$

2. El retículo

(H)



no es distributivo, por las igualdades

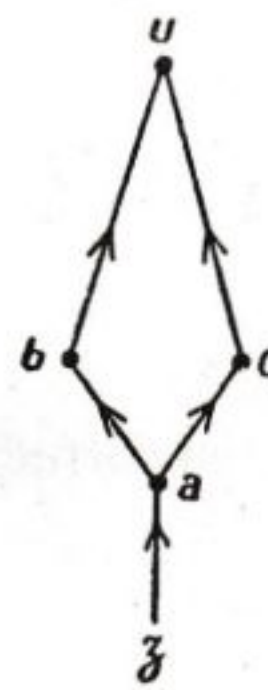
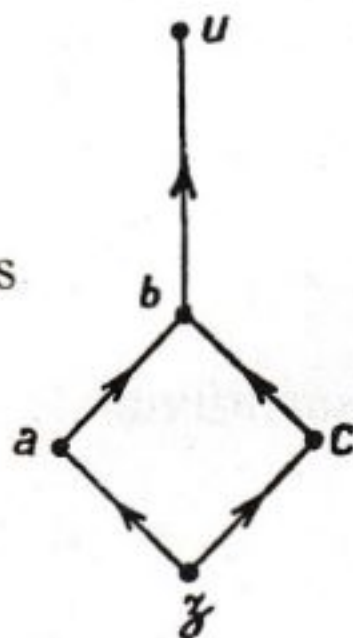
$$\begin{aligned} a \vee (b \wedge c) &= a \vee z = a, \\ (a \vee b) \wedge (a \vee c) &= b \wedge u = b, \quad a \neq b. \end{aligned}$$

Observación. — Con 5 elementos distintos formando un conjunto ordenado, los únicos retículos posibles (puesto que es preciso tener un elemento z y un elemento u) son, además de los dos precedentes y sus permutaciones respecto de los elementos a, b, c ,

la cadena



y los retículos



Se comprueba sin dificultad que la cadena y estos retículos son retículos distributivos. Estos son, pues, *los únicos retículos distributivos de cinco elementos*.

Inversamente, consideremos un conjunto E con dos leyes de composición interna *idempotentes* (I), *conmutativas* (II), *asociativas* (III), y ligadas por la *ley de absorción* (IV). Con la ayuda de una de estas dos leyes, se pueden definir dos relaciones de orden opuestas. Hemos visto, por ejemplo, que se tiene un *inf-semirretículo* con $\inf(a, b) = a \top b$, y la relación de orden es definida por

$$a \leqslant b \text{ si } a \top b = a$$

Tomemos, pues, aquí $a \leqslant b$ si $a \wedge b = a$.

Demostremos ahora que este conjunto es un retículo. En efecto:

$$a \wedge (a \vee b) = a$$

en virtud de la ley de absorción, y esto implica:

$a \leq (a \vee b)$, y también, en virtud de la conmutatividad $b \leq (a \vee b)$.

El conjunto es, pues, filtrante superiormente.

Pero la ley de absorción muestra que:

$$a \wedge b = a \quad \text{implica} \quad a \vee b = (a \wedge b) \vee b = b \vee (b \wedge a) = b$$

e inversamente:

$$a \vee b = b \quad \text{implica} \quad a \wedge b = a \wedge (a \vee b) = a.$$

Las relaciones:

$$a \wedge b = a, \quad a \vee b = b$$

tienen pues lugar al mismo tiempo y la relación de orden puede también escribirse así:

$$\underline{a \leq b \quad \text{si} \quad a \vee b = b.}$$

Sea entonces μ tal que $a \leq \mu$ y $b \leq \mu$. Se deduce:

$$a \vee \mu = \mu \quad \text{y} \quad b \vee \mu = \mu.$$

Luego, en virtud de la asociatividad:

$$(a \vee b) \vee \mu = \mu, \quad a \vee b \leq \mu.$$

Dos elementos cualesquiera a, b tienen pues un mayorante mínimo:

$$\sup(a, b) = a \vee b$$

y el conjunto ordenado E es efectivamente un retículo.

Observaciones. — 1. $a \leq b$ es equivalente a $a \wedge b = a$ o $a \vee b = b$, y esta propiedad implica en virtud de la idempotencia, de la conmutatividad y de la asociatividad de $\wedge$ y de $\vee$:

$$(a \wedge x) \wedge (b \wedge x) = a \wedge x, \quad (a \vee x) \vee (b \vee x) = b \vee x,$$

es decir,

$$a \wedge x \leq b \wedge x \quad \text{y} \quad a \vee x \leq b \vee x$$

para todo x , lo que se expresa diciendo que $\wedge$ y $\vee$ son *isótonas* para la relación de orden $\leq$.

2. En un conjunto E con dos leyes de composición internas, los axiomas de asociatividad, conmutatividad, idempotencia y ley de absorción no son independientes; la idempotencia es consecuencia de la ley de absorción que liga las dos leyes de composición asociativas y conmutativas.

3. Los axiomas I a IV permanecen invariables si se cambia $\vee$ y $\wedge$.

Si se hace esta operación, $a \wedge b = a$ se convierte en $a \vee b = a$, lo que reemplaza el orden elegido por el orden opuesto (puesto que $a \wedge b = a$ y $a \vee b = b$ son equivalentes), luego:

En un retículo toda propiedad que sea consecuencia lógica de los axiomas I, II, III, IV y de la elección de la relación de orden: $a \leq b$ si $a \wedge b = a$ permanece válida cuando se permutan entre sí los dos signos $\wedge$ y $\vee$ al tiempo que los $\leq$ y $\geq$ también entre sí. Tal es el enunciado del llamado principio de dualidad.

Pasemos revista rápidamente a los principales tipos de retículos.

§ 6. Retículos distributivos; retículos complementados

Recordemos que un retículo distributivo es un retículo $\mathcal{G}$ en el cual, además de los axiomas habituales, se tiene la *distributividad* de cada una de las operaciones con respecto a la otra:

$$(V) \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \quad \forall a, b, c \in \mathcal{G},$$

$$(V') \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), \quad \forall a, b, c \in \mathcal{G}.$$

Naturalmente en todo retículo, las relaciones $b \leq b \vee c$, $c \leq b \vee c$ implican

$$a \wedge b \leq a \wedge (b \vee c) \quad \text{y} \quad a \wedge c \leq a \wedge (b \vee c)$$

de donde

$$(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$$

y lo mismo

$$b \wedge c \leq b \quad \text{y} \quad b \wedge c \leq c$$

implican

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c).$$

Observación. — *Los axiomas V y V' no son independientes: cada uno implica al otro.*

Supongamos que $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, $\forall x, y, z \in \mathcal{C}$.
Calculemos entonces:

$$\alpha = (x \vee y) \wedge (x \vee z) = [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z].$$

Pero, en virtud de la ley de absorción, tenemos

$$\begin{aligned} \alpha &= x \vee [(x \vee y) \wedge z] = x \vee [z \wedge (x \vee y)] \\ &= x \vee [(z \wedge x) \vee (z \wedge y)] \\ &= [x \vee (z \wedge x)] \vee (z \wedge y) \\ &= x \vee (z \wedge y) \end{aligned} \quad \text{c.q.d.}$$

Si se supone ahora que $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, el cálculo de $\beta = (x \wedge y) \vee (x \wedge z)$ es dual del precedente y da

$$\beta = x \wedge (z \vee y).$$

Luego: *el sistema de axiomas que caracteriza a los retículos distributivos es ipsodual, por lo que en estos retículos es válido el principio de dualidad.*

Ejemplos. — 1.º Hemos visto ya que una cadena es un retículo distributivo.

2.º $\mathcal{P}(E)$ con las operaciones $\cap$ y $\cup$, reunión e intersección en el sentido de la teoría de conjuntos, es un retículo distributivo.

Incluso, aquí, puede afirmarse más: este retículo es completo y verifica las *leyes distributivas generales*. Estas leyes, que pueden o no ser satisfechas en un retículo distributivo completo $\mathcal{C}$ se escriben para todo $\mathcal{A} \subset \mathcal{C}$ y $b \in \mathcal{C}$:

$$\begin{aligned} (V^*) \quad & (\bigvee_{a \in \mathcal{A}} a) \wedge b = \bigvee_{a \in \mathcal{A}} (a \wedge b) \\ (V'^*) \quad & (\bigwedge_{a \in \mathcal{A}} a) \vee b = \bigwedge_{a \in \mathcal{A}} (a \vee b) \end{aligned}$$

Pero es preciso advertir que V^* no implica V'^* .

3.º El retículo de los enteros con

$$a \vee b = \text{m.c.m. } (a, b) \text{ y } a \wedge b = \text{m.c.d. } (a, b)$$

es distributivo. (Se ve, por ejemplo, utilizando las descomposiciones en factores primos y aplicando la distributividad de las cadenas.)

4.º El retículo de los filtros de un conjunto E es un retículo distributivo. Sean $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ tres filtros de E . Sabemos que

$$\mathcal{F}_1 \wedge (\mathcal{F}_2 \vee \mathcal{F}_3) = \{ F_1 \cup (F_2 \cap F_3); F_1 \in \mathcal{F}_1, F_2 \in \mathcal{F}_2, F_3 \in \mathcal{F}_3 \}.$$

Pero todo elemento $F_1 \cup (F_2 \cap F_3) = (F_1 \cup F_2) \cap (F_1 \cup F_3)$ pertenece a $(\mathcal{F}_1 \wedge \mathcal{F}_2) \vee (\mathcal{F}_1 \wedge \mathcal{F}_3)$. Así, tenemos ya:

$$\mathcal{F}_1 \wedge (\mathcal{F}_2 \vee \mathcal{F}_3) \subseteq (\mathcal{F}_1 \wedge \mathcal{F}_2) \vee (\mathcal{F}_1 \wedge \mathcal{F}_3)$$

es decir en el retículo de los filtros,

$$\mathcal{F}_1 \wedge (\mathcal{F}_2 \vee \mathcal{F}_3) \leq (\mathcal{F}_1 \wedge \mathcal{F}_2) \vee (\mathcal{F}_1 \wedge \mathcal{F}_3),$$

y como en todo retículo se tiene

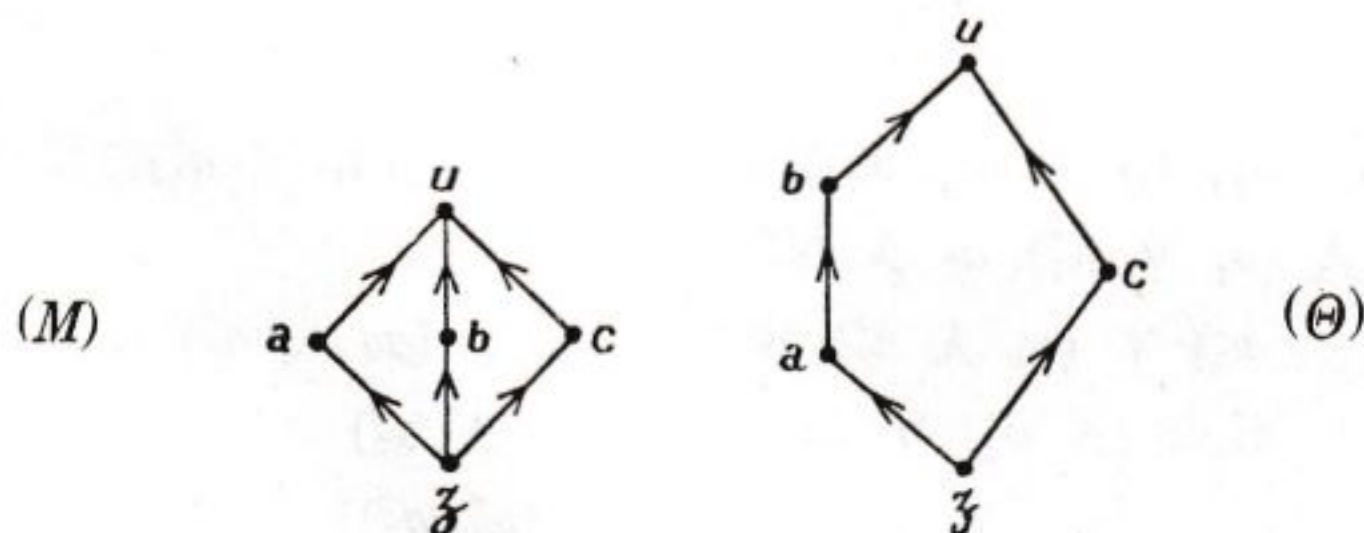
$$(\mathcal{F}_1 \wedge \mathcal{F}_2) \vee (\mathcal{F}_1 \wedge \mathcal{F}_3) \leq \mathcal{F}_1 \wedge (\mathcal{F}_2 \vee \mathcal{F}_3)$$

se tiene, en efecto,

$$(\mathcal{F}_1 \wedge \mathcal{F}_2) \vee (\mathcal{F}_1 \wedge \mathcal{F}_3) = \mathcal{F}_1 \wedge (\mathcal{F}_2 \vee \mathcal{F}_3).$$

Propiedades. — *Todo subretículo de un retículo distributivo es un retículo distributivo; esto es evidente, por la definición de subretículo y de la distributividad. Resulta de ello:*

Si un retículo es distributivo, no contiene subretículos isomorfos a ninguno de los retículos (M) y (Θ) del diagrama siguiente (no distributivos, como se ha visto en § 5):



Tenemos pues una condición necesaria para que un retículo sea distributivo. Consideremos ahora, en un retículo *distributivo*, tres elementos a, b, c ligados por las relaciones

$$\begin{aligned} c \wedge a &= c \wedge b \\ c \vee a &= c \vee b \end{aligned}$$

Tenemos

$$\begin{aligned} a &= a \vee (c \wedge a) = a \vee (c \wedge b) = (a \vee c) \wedge (a \vee b) \\ b &= b \vee (c \wedge b) = b \vee (c \wedge a) = (b \vee c) \wedge (b \vee a), \end{aligned}$$

de donde

$$a = b.$$

Así, todo retículo distributivo verifica la condición

$$(A) \quad \left. \begin{array}{c} c \wedge a = c \wedge b \\ \text{y} \\ c \vee a = c \vee b \end{array} \right\} \text{ implican } a = b.$$

Observemos además que esta nueva condición *necesaria* (A) implica inmediatamente la condición necesaria establecida precedentemente (inexistencia de subretículos de cinco elementos de los tipos Θ y M).

Veremos en el § 8 que cada una de estas dos condiciones es no solamente necesaria, sino también *suficiente*, para que un retículo sea distributivo.

El retículo producto de dos retículos distributivos es distributivo:

$$\mathcal{G}_1 \times \mathcal{G}_2 = \{ (a_1, a_2) ; a_1 \in \mathcal{G}_1, a_2 \in \mathcal{G}_2 \}$$

con:

$$\begin{aligned} (a_1, a_2) \wedge (a'_1, a'_2) &= (a_1 \wedge a'_1, a_2 \wedge a'_2) \\ (a_1, a_2) \vee (a'_1, a'_2) &= (a_1 \vee a'_1, a_2 \vee a'_2). \end{aligned}$$

Se tiene, por la distributividad en $\mathcal{G}_1$ y $\mathcal{G}_2$:

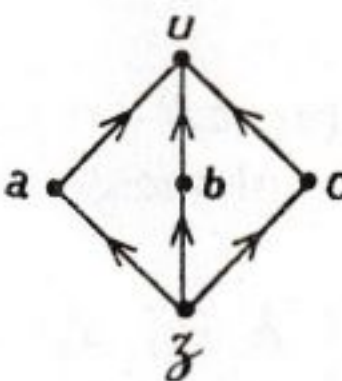
$$\begin{aligned} (a_1, a_2) \wedge [(a'_1, a'_2) \vee (a''_1, a''_2)] &= (a_1, a_2) \wedge [(a'_1 \vee a''_1), (a'_2 \vee a''_2)] \\ &= [a_1 \wedge (a'_1 \vee a''_1), a_2 \wedge (a'_2 \vee a''_2)] \\ &= [(a_1 \wedge a'_1) \vee (a_1 \wedge a''_1), (a_2 \wedge a'_2) \vee (a_2 \wedge a''_2)] \\ &= (a_1 \wedge a'_1, a_2 \wedge a'_2) \vee (a_1 \wedge a''_1, a_2 \wedge a''_2) \\ &= [(a_1, a_2) \wedge (a'_1, a'_2)] \vee [(a_1, a_2) \wedge (a''_1, a''_2)] \quad \text{c.q.d.} \end{aligned}$$

En un retículo con elemento nulo, z , y elemento universal, u , se llama *complemento* de un elemento a a todo elemento a' que verifica las dos igualdades

$$a \wedge a' = z \quad \text{y} \quad a \vee a' = u.$$

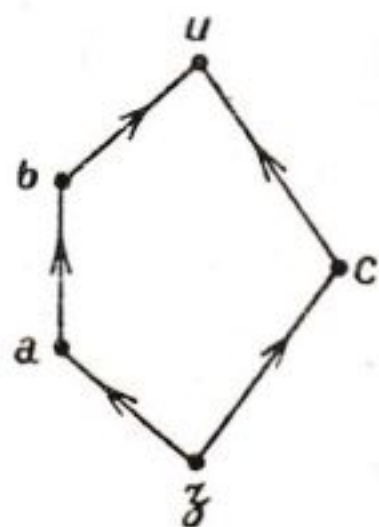
Si a' es complemento de a , a es complemento de a' .

Ejemplos. — 1. En el retículo a b c z es complemento de u ; cada



uno de los elementos a , b , c tiene por complemento los otros dos.

2. En el retículo



c es complemento de a y b .

Teorema 1. — *En un retículo distributivo, el complemento de a , si existe, es único.*

Supongamos que en un retículo distributivo $\mathfrak{L}$, dos elementos a' , a'' fuesen complemento de a y, por lo tanto, verificasen

$$\begin{array}{ll} a \wedge a' = z & \text{y} \quad a \wedge a'' = z \\ a \vee a' = u & \text{y} \quad a \vee a'' = u \end{array}$$

De ello resulta:

$$\begin{array}{l} a \wedge a' = a \wedge a'' \\ a \vee a' = a \vee a'' \end{array}$$

de donde, según la segunda condición necesaria para que un retículo sea distributivo:

$$a' = a''$$

Definición. — Se llama *retículo complementado* un retículo con elemento cero, z , y elemento universal, u , en el cual todo elemento x tiene al menos un complemento x' .

En un retículo distributivo y complementado, todo elemento x tiene un complemento x' y uno solo.

Teorema 2. — *El producto de dos retículos complementados $\mathcal{A}_1$, y $\mathcal{A}_2$ es u*

retículo complementado.

Es claro que todo elemento (a_1, a_2) del retículo producto admite por complemento (a'_1, a'_2) , donde a'_i es un complemento de a_i en $\mathcal{A}_i$. Tenemos en efecto:

$$(a_1, a_2) \wedge (a'_1, a'_2) = (z_1, z_2)$$

$$(a_1, a_2) \vee (a'_1, a'_2) = (u_1, u_2)$$

donde z_i, u_i son respectivamente el elemento cero y el elemento universal de $\mathcal{A}_i$, (z_1, z_2) y (u_1, u_2) son por consiguiente elemento cero y elemento universal del retículo producto.

Ejemplos. — 1. Si E es un conjunto cualquiera, el conjunto $\mathfrak{F}(E)$ de las partes de E es complementado; se tiene

$$A' = \complement_E A.$$

2. El retículo formado por los filtros de E con $\mathfrak{F}(E)$ no es complementado. Este retículo admite el elemento cero $\{E\}$ y el elemento universal $\mathfrak{F}(E)$. Consideremos el filtro Φ , conjunto de las partes complementarias de las partes finitas de E , (visto en pág. 196, ejemplo 2) y supongamos que $\mathcal{K}$ sea un filtro complementario de Φ . Una parte $H \in \mathcal{K}$ debe en primer lugar ser tal que

$$H \cup F = E, \quad \forall F \in \Phi.$$

H debe pues contener el complementario $\complement_E F$, cualquiera que sea $F \in \Phi$; H debe pues contener toda parte finita de E , en particular todo elemento de E , lo que exige $H = E$, $\mathcal{K} = \{E\}$.

Pero entonces, tendremos

$$\{E\} \vee \Phi = \Phi \neq \mathfrak{F}(E)$$

El filtro complementario $\mathcal{K}$ no existe pues, y el retículo de los filtros no es complementado.

Sin embargo, este retículo admite un subretículo, *el retículo de los filtros principales*, y éste sí es complementado.

Sea $\mathcal{F}(A)$ el filtro principal engendrado por A , conjunto de las partes de E que contienen a A . Tenemos

$$\mathcal{F}(A) \vee \mathcal{F}(B) = \mathcal{F}(A \cap B)$$

$$\mathcal{F}(A) \wedge \mathcal{F}(B) = \mathcal{F}(A \cup B)$$

lo que se expresa diciendo que la aplicación biyectiva $A \rightarrow \mathcal{F}(A)$ es un *isomorfismo-anti*¹ entre $\mathcal{I}(E)$ y el retículo de los filtros principales. Este retículo es complementado, como $\mathcal{I}(E)$ puesto que tenemos

$$\mathcal{F}(A) \vee \mathcal{F}(\mathcal{C}_E A) = \mathcal{I}(E) = \mathcal{F}(\emptyset)$$

$$\mathcal{F}(A) \wedge \mathcal{F}(\mathcal{C}_E A) = \{E\} = \mathcal{F}(E).$$

§ 7. Retículos de Boole

Definición. — Se llama *retículo de Boole* un retículo distributivo y complementado.

Teorema 1. — En un retículo de Boole, se tiene

$$(a \wedge b)' = a' \vee b', \quad (a \vee b)' = a' \wedge b'.$$

La comprobación es fácil; demostremos por ejemplo la primera relación:

$$\begin{aligned} (a \wedge b) \wedge (a' \vee b') &= (a' \wedge a \wedge b) \vee (b' \wedge b \wedge a) \\ &= (z \wedge b) \vee (z \wedge a) = z \vee z = z; \\ (a \wedge b) \vee (a' \vee b') &= (a \vee a' \vee b') \wedge (a' \vee b' \vee b) \\ &= (u \vee b') \wedge (a' \vee u) = u \wedge u = u. \end{aligned}$$

Se ha visto ya que el retículo $\mathcal{I}(E)$ de las partes de un conjunto E es distributivo y complementado; es, pues, un retículo de Boole.

El retículo constituido por dos elementos a_1 y b_1 con $a_1 < b_1$ es distributivo y complementado: $a_1' = b_1$. Luego el producto de p retículos $\mathcal{C}_i$ de este tipo $\mathcal{C}_i = \{a_i, b_i; a_i < b_i\}$ es también un retículo de Boole $\mathcal{C}$ cuyos elementos son:

$$x = (x_1, \dots, x_i, \dots, x_p) \quad \text{con} \quad x_i = a_i \quad \text{o} \quad x_i = b_i.$$

Así, $\mathcal{C}$ tiene 2^p elementos. Sea $P = \{1, 2, \dots, p\}$. $\mathcal{C}$ es isomorfo a $\mathcal{I}(P)$. En efecto, se puede hacer corresponder biunívocamente $\mathcal{C}$ y $\mathcal{I}(P)$ asociando

¹ Como realmente es un isomorfismo preferimos traducir así la locución "anti-isomorphisme" del original. En español con anti-isomorfismo se indica la circunstancia de que $a \rightarrow a'$ y $b \rightarrow b'$ impliquen $ab \rightarrow b'a'$. (N. del T.)

$x \in \mathcal{G}$, $B_x \subseteq P$ constituido por los índices de los elementos x_i de x que son de los b_i , e inversamente a $B \subseteq P$ asociarle el elemento x de $\mathcal{G}$ definido por:

$$\begin{aligned} x_i &= b_i & \text{para } i \in B, \\ x_j &= a_j & \text{para } j \notin B. \end{aligned}$$

Y para que sea $x \leq y$ en $\mathcal{G}$ es decir $x_i \leq y_i$ en $\mathcal{G}_i$ cualquiera que sea $i \in \{1, 2, \dots, n\}$, es necesario y suficiente que sea $B_x \subseteq B_y$ en $\mathcal{I}(P)$.

Teorema 2. — *Un reticulo de Boole $\mathcal{G}$ es un anillo conmutativo, idempotente con elemento unidad, o anillo de Boole.*

Consideremos en efecto la ley de composición interna definida en el reticulo de Boole por:

$$(1) \quad a + b = (a' \wedge b') \vee (a \wedge b).$$

Utilizando la distributividad de $\vee$ respecto a $\wedge$, se tiene:

$$\begin{aligned} a + b &= [(a' \wedge b') \vee a] \wedge [(a' \wedge b') \vee b] \\ &= (a' \vee a) \wedge (b' \vee a) \wedge (a' \vee b) \wedge (b' \vee b) \end{aligned}$$

es decir

$$(2) \quad a + b = (a' \vee b) \wedge (a \vee b').$$

Esta adición es visiblemente *conmutativa*.

Para demostrar que es *asociativa*, observemos en primer lugar que según (2) tenemos:

$$(a + b)' = (a \wedge b') \vee (a' \wedge b)$$

de donde, según (1),

$$\begin{aligned} (a + b) + c &= [(a + b)' \wedge c'] \vee [(a + b) \wedge c] \\ &= \{[(a \wedge b') \vee (a' \wedge b)] \wedge c'\} \vee \{[(a' \wedge b') \vee (a \wedge b)] \wedge c\} \end{aligned}$$

y finalmente

$$(3) \quad (a + b) + c = (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (a \wedge b \wedge c)$$

que es simétrica en a, b, c , de donde

$$(a + b) + c = a + (b + c).$$

Tenemos por otra parte, según (1),

$$a + u = (a' \wedge z) \vee (a \wedge u) = z \vee a = a$$

por consiguiente u es el elemento neutro para la adición considerada.

Además, según (1) es siempre

$$a + a = a' \vee a = u$$

a es, pues, su propio opuesto, todo elemento es involutivo, y el retículo de Boole $\mathfrak{G}$ es, para la adición considerada, un *grupo abeliano*. En el caso particular del retículo de Boole $\mathfrak{F}(E)$, $A + B$ es el conjunto de los elementos de E que o bien pertenecen a la vez a A y B , o bien no pertenecen ni a A ni a B ; este conjunto se llama *suma simétrica* de A y B .

Para hacer de $\mathfrak{G}$ un anillo, tomemos, además de la adición precedente, una multiplicación confundida con la ley $\vee$:

$$a \cdot b = a \vee b.$$

Sabemos que esta multiplicación es asociativa, conmutativa e idempotente y que admite z como elemento unidad. Para establecer ahora que es un anillo, nos basta probar que la multiplicación es *distributiva* respecto a la adición. Ahora bien, tenemos según (2):

$$(a + b) c = [(a' \vee b) \wedge (a \vee b')] \vee c = (a' \vee b \vee c) \wedge (a \vee b' \vee c),$$

mientras que

$$\begin{aligned} ac + bc &= (a \vee c) + (b \vee c) \\ &= \{ (a \vee c)' \vee (b \vee c) \} \wedge \{ (b \vee c)' \vee (a \vee c) \} \end{aligned}$$

Las dos llaves se deducen la una de la otra por cambio de a y b y así tenemos, por ejemplo

$$\begin{aligned} (a \vee c)' \vee (b \vee c) &= (a' \wedge c') \vee b \vee c \\ &= b \vee [(a' \vee c) \wedge (c' \vee c)] = a' \vee b \vee c. \end{aligned}$$

La distributividad resulta de aquí y, en consecuencia de todo esto, $\mathfrak{G}$ con las leyes de composición $+$ y $\cdot$, es un anillo de Boole que designaremos por B .

Observación. — Se obtiene también de un retículo de Boole $\mathcal{C}$ un anillo de Boole $\mathcal{B}'$ por el procedimiento *dual*, es decir tomando como suma

$$a + b = (a' \vee b') \wedge (a \vee b) = (a' \wedge b) \vee (a \wedge b')$$

lo que en $\mathcal{P}(E)$, corresponde a la *diferencia simétrica*, conjunto de los elementos de E que pertenecen a uno, y sólo a uno, de los conjuntos A, B ; y como producto

$$ab = a \wedge b.$$

Teorema 3. — *Los ideales del anillo de Boole $\mathcal{B}$ son estables para la ley $\wedge$.*

Se sabe, en efecto, que un ideal $\mathcal{J}$ en un anillo es un subgrupo aditivo y una parte lícita para la multiplicación. Luego, si a y b son dos elementos de $\mathcal{J}$, se tiene $a + b \in \mathcal{J}$, pero también $a \vee b \in \mathcal{J}$ y por consiguiente

$$a + b + (a \vee b) \in \mathcal{J}.$$

Ahora bien, la fórmula (3) que da $a + b + c$, aplicada al caso $c = a \vee b$, se reduce a

$$a + b + (a \vee b) = a \wedge b$$

pues se tiene

$$c' = a' \wedge b',$$

de donde

$$a \wedge b' \wedge c' = a' \wedge b \wedge c' = a' \wedge b' \wedge c = z$$

mientras que

$$a \wedge b \wedge c = a \wedge b.$$

En el caso particular, pero fundamental, del retículo de Boole de las partes de un conjunto E , hemos estudiado con detalle, bajo el nombre de *filtros*, tales conjuntos estables para la intersección y lícitos para la reunión.

Los retículos de Boole tienen todas las propiedades algebraicas del retículo $\mathcal{P}(E)$ que intervienen en el estudio de los filtros que hemos hecho, así como en el estudio de las familias de Moore. Se pueden pues considerar, en un retículo de Boole cualquiera $\mathcal{C}$, y llamar *filtros* de $\mathcal{C}$, los subconjuntos $\mathcal{F}$ tales que

- 1) x_1 y $x_2 \in \mathcal{F}$ implican $x_1 \wedge x_2 \in \mathcal{F}$,
- 2*) $x \in \mathcal{F}, t \in \mathcal{C}$ implican $x \vee t \in \mathcal{F}$,

ó

- 2) $x \in \mathcal{F}, y \in \mathcal{G}, x \leq y$ implican $y \in \mathcal{F}$,
 3) $z \notin \mathcal{F}$ (para que $\mathcal{F}$ sea diferente de $\mathcal{G}$).

Las propiedades establecidas para los filtros y las familias de Moore de $\mathcal{T}(E)$ son válidas para los filtros y las familias de Moore de cualquier retículo de Boole $\mathcal{G}$. En particular, los filtros de $\mathcal{G}$ y el mismo $\mathcal{G}$ forman una familia de Moore, llamada *familia de los filtros* del retículo $\mathcal{G}$ y se puede enunciar según el teorema 3:

Los ideales del anillo de Boole $\mathcal{B}$ correspondiente a un retículo de Boole $\mathcal{G}$ son filtros de $\mathcal{G}$.

Recíprocamente, todo filtro $\mathcal{F}$ de un retículo de Boole $\mathcal{G}$ es un ideal del anillo de Boole correspondiente $\mathcal{B}$.

En efecto, sabemos ya que $\mathcal{F}$ es lícito para $\vee$; demostremos que $\mathcal{F}$ es un grupo aditivo.

Sean a y $b \in \mathcal{F}$; puesto que $a \leq a \vee b'$, se tiene: $a \vee b' \in \mathcal{F}$; e igualmente $b \vee a' \in \mathcal{F}$; pero un filtro es estable para $\wedge$, luego se tiene:

$$(a \vee b') \wedge (b \vee a') = a + b \in \mathcal{F}$$

Luego $\mathcal{F}$ es estable para la adición; $\mathcal{F}$ contiene el elemento máximo u , que es elemento neutro para la adición; y puesto que el opuesto de todo elemento es el mismo elemento, $\mathcal{F}$ es un subgrupo.

En particular los filtros de $\mathcal{T}(E)$ son los ideales del anillo de Boole $\mathcal{T}(E)$. Un filtro no contiene a $\emptyset$, elemento neutro para $\vee$ (multiplicación del anillo de Boole), luego es un ideal propio; el filtro degenerado $\mathcal{T}(E)$ es el ideal impropio constituido por el anillo completo.

Acabamos pues de demostrar, que *todo retículo de Boole puede ser estructurado como anillo de Boole, siendo los filtros del retículo los ideales del anillo. Recíprocamente, todo anillo $\mathcal{A}$ idempotente con elemento unidad 1 es un anillo de Boole, y puede ser ordenado en retículo de Boole, de manera que el anillo de Boole asociado a este retículo por el procedimiento antedicho sea el anillo de partida $\mathcal{A}$.*

Es preciso demostrar primero que:

Todo anillo idempotente es conmutativo.

Lema. — *Todo anillo idempotente $\mathcal{A}$ es de característica 2.*

Se tiene en efecto:

$$(a + b)(a + b) = (a + b)$$

en virtud de la idempotencia, pero la distributividad da:

$$(a + b)(a + b) = a^2 + ba + ab + b^2$$

y la idempotencia implica finalmente

$$(4) \quad 0 = ab + ba$$

Para $b = a$, la igualdad (4) da

$$2a = 0, \quad \forall a \in \mathcal{A};$$

el anillo $\mathcal{A}$ es pues un anillo de característica 2.

Sentado esto (4), se escribe

$$2ab = ab + ba$$

es decir

$$ab = ba,$$

por lo que el anillo $\mathcal{A}$ es conmutativo.

Consideremos entonces en $\mathcal{A}$ las dos leyes de composición $\vee$ y $\wedge$ definidas por

$$(5) \quad a \vee b = ab, \quad a \wedge b = a + b + ab.$$

La ley $\vee$ es por hipótesis, asociativa, conmutativa e idempotente; la ley $\wedge$ es conmutativa; es asociativa, pues

$$\begin{aligned} (a \wedge b) \wedge c &= (a \wedge b) + c + (a \wedge b) c \\ &= a + b + ab + c + (a + b + ab) c \\ &= a + b + c + ab + bc + ca + abc, \end{aligned}$$

expresión simétrica, lo que implica

$$(a \wedge b) \wedge c = a \wedge (b \wedge c).$$

La ley $\wedge$ es además idempotente, puesto que

$$a \wedge a = a + a + a^2 = a^2 = a.$$

Las dos operaciones $\wedge$ y $\vee$ verifican la ley de absorción:

$$a \vee (a \wedge b) = a(a + b + ab) = a^2 + ab + a^2b = a + 2ab = a,$$

$$a \wedge (a \vee b) = a + ab + a^2b = a + 2ab = a.$$

$\mathcal{A}$ con las dos leyes $\wedge$ y $\vee$, es por consiguiente un retículo, que designaremos por $\mathfrak{C}$.

Este retículo $\mathfrak{C}$ es *distributivo*; tenemos en efecto

$$a \vee (b \wedge c) = a(b + c + bc) = ab + ac + abc,$$

y

$$(a \vee b) \wedge (a \vee c) = ab + ac + a^2bc = ab + ac + abc.$$

Como ya sabemos, esta distributividad implica la otra; aquí, por otra parte, se verifica inmediatamente que

$$\begin{aligned} (a \wedge b) \vee (a \wedge c) &= (a + b + ab)(a + c + ac) \\ &= a + bc + abc \\ &= a \wedge bc = a \wedge (b \vee c). \end{aligned}$$

La *relación de orden* del retículo $\mathfrak{C}$ está definida por

$$a \leqslant b \quad \text{si} \quad a \wedge b = a$$

$$\text{o si} \quad a \vee b = b \quad \text{es decir} \quad ab = b.$$

El elemento unidad 1 de $\mathcal{A}$, tal que $1 \cdot b = 1 \vee b = b$, $\forall b \in \mathfrak{C}$ es elemento cero, z , del retículo $\mathfrak{C}$ (es decir elemento mínimo). El elemento 0 de $\mathcal{A}$ (neutro para la adición), tal que

$$0 \wedge b = 0 + b + 0b = b \quad \forall b \in \mathfrak{C}$$

es *elemento universal* u , del retículo $\mathfrak{C}$.

En fin, $\mathcal{C}$ es *complementado* y por consiguiente es un *retículo de Boole*. Pongamos en efecto

$$a' = 1 + a.$$

Tenemos

$$\begin{aligned} a' \wedge a &= (1 + a) \wedge a = 1 + a + a + (1 + a) a = 1 = z, \\ a' \vee a &= (1 + a) a = 0 = u. \end{aligned}$$

Además, el anillo de Boole $\mathcal{B}$, construido a partir de $\mathcal{C}$ siguiendo el método del teorema 2, coincide con $\mathcal{A}$; de las igualdades

$$\begin{aligned} a \wedge b &= a + b + ab, \\ a' \wedge b' &= 1 + a + 1 + b + (1 + a)(1 + b) = 1 + ab, \end{aligned}$$

se deduce en efecto

$$(a \wedge b) \vee (a' \wedge b') = (a + b + ab)(1 + ab) = a + b.$$

En resumen hemos establecido el teorema siguiente:

Teorema 4. — *Todo anillo idempotente con elemento unidad 1 es conmutativo, luego es un anillo de Boole $\mathcal{B}$; además, $\mathcal{B}$ es un retículo de Boole con respecto a las leyes de composición $\vee$ y $\wedge$ definidas por*

$$(5) \quad a \vee b = ab, \quad a \wedge b = a + b + ab.$$

Indiquemos algunas propiedades importantes de los ideales de un anillo de Boole $\mathcal{B}$; si x es un elemento cualquiera de $\mathcal{B}$, se tiene

$$x(1 - x) = x - x^2 = x - x = 0$$

y por consiguiente, si $\mathfrak{m}$ es un ideal cualquiera de $\mathcal{B}$,

$$x(1 - x) \in \mathfrak{m}.$$

Resulta de aquí que, si $\mathfrak{p}$ es un ideal primo distinto de $\mathcal{B}$, para todo elemento x de $\mathcal{B}$, uno de los elementos x , $1 - x$ pertenece a $\mathfrak{p}$, y uno solo, pues de otro modo tendríamos $1 \in \mathfrak{p}$, luego $\mathfrak{p} = \mathcal{B}$.

Consecuencia: todo ideal primo $\mathfrak{p} \neq \mathcal{B}$ es maximal.

Sea en efecto $\mathfrak{m}$ un ideal que verifica

$$\mathfrak{p} \subset \mathfrak{m} \subseteq \mathfrak{B},$$

donde la primera inclusión es estricta: sea entonces m un elemento de $\mathfrak{m}$ no perteneciente a $\mathfrak{p}$. Tenemos

$$1 - m \in \mathfrak{p} \subseteq \mathfrak{m}$$

luego $1 \in \mathfrak{m}$ y $\mathfrak{m} = \mathfrak{B}$, $\mathfrak{p}$ es maximal.

Por otra parte, *todo ideal $\mathfrak{p} \neq \mathfrak{B}$ tal que, cualquiera que sea $x \in \mathfrak{B}$, uno de los elementos $x, 1 - x$ pertenece a $\mathfrak{p}$, es un ideal primo.*

Sea en efecto $xy \in \mathfrak{p}, x \notin \mathfrak{p}$. Entonces $1 - x \in \mathfrak{p}$, de donde $(1 - x)y = y - xy \in \mathfrak{p}$ y por consiguiente $y \in \mathfrak{p}$.

Podemos enunciar:

Teorema 5. — *Para un ideal $\mathfrak{p}$ de un anillo de Boole $\mathfrak{B}$, las tres propiedades siguientes son equivalentes:*

- a) $\mathfrak{p}$ es un ideal primo diferente de $\mathfrak{B}$;
- b) $\mathfrak{p}$ es maximal;
- c) *cualquiera que sea $x \in \mathfrak{B}$, uno, y sólo uno, de los dos elementos $x, 1 - x$ pertenece a $\mathfrak{p}$.*

La caracterización de un ideal maximal de un retículo de Boole por la propiedad c) permite formular un resultado clásico sobre los filtros.

Se llama *ultrafiltro* a un filtro propio maximal.

Teorema 6. — *Un filtro $\mathcal{F}$ de partes de un conjunto E es un ultrafiltro si, y sólo si, para toda partición de E en dos clases X e Y , una de las clases X o Y pertenece a $\mathcal{F}$.*

En $\mathcal{P}(E)$ considerado como anillo de Boole $\mathfrak{B}$, la multiplicación no es otra que la reunión de partes, el elemento unidad es el conjunto vacío $\emptyset$. $\mathcal{F}$ es un ultrafiltro, es decir un ideal maximal de $\mathfrak{B}$, si cualquiera que sea $X \in \mathfrak{B}$, uno de los elementos $X, \emptyset - X$ pertenece a $\mathcal{F}$, y solamente en este caso. Ahora bien, siendo $\mathfrak{B}$ de característica 2, tenemos $\emptyset - X = \emptyset + X$ y según la definición (2) de la adición

$$\emptyset + X = (\mathcal{C}_E \emptyset \cup X) \cap (\emptyset \cup \mathcal{C}_E X) = E \cap \mathcal{C}_E X = \mathcal{C}_E X = Y.$$

§ 8. Retículos modulares

En todo retículo $\mathcal{C}$, es sabido que para tres elementos cualesquiera x, y, z se tiene:

$$(1) \quad x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z).$$

Se deduce inmediatamente que:

$$(2) \quad x \leq z \quad \text{implica} \quad x \vee (y \wedge z) \leq (x \vee y) \wedge z,$$

y la igualdad vale para $z = x$ según la ley de absorción.

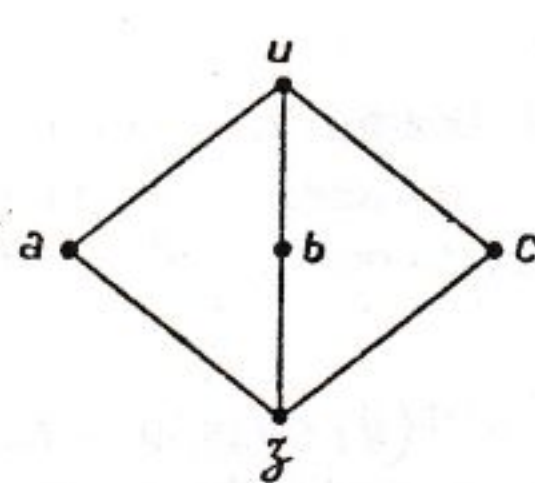
Definición. — Un retículo $\mathcal{C}$ se llama *modular* si:

$$(3) \quad x \leq z \quad \text{implica} \quad x \vee (y \wedge z) = (x \vee y) \wedge z.$$

Todo retículo distributivo es modular, pues la igualdad

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z),$$

con $x \leq z$, da la relación modular (3).

Notemos que el retículo definido por el diagrama  que

no es distributivo, es modular. En efecto, para $x = z$, la condición (3) se reduce a la igualdad; si se toma por ejemplo $x = a, z = u$, se tiene:

$$x \vee (y \wedge z) = a \vee (y \wedge u) = a \vee y,$$

$$(x \vee y) \wedge z = (a \vee y) \wedge u = a \vee y$$

y (3) se cumple; ocurre lo mismo para $x = b$ ó c ; en fin, para $x = z = u$, se tiene también la igualdad.

Observación. — *La propiedad de modularidad se conserva por dualidad, pues la propiedad dual*

$$x \geq z \quad \text{implica} \quad x \wedge (y \vee z) = (x \wedge y) \vee z$$

es decir

$$z \leq x \quad \text{implica} \quad z \vee (x \wedge y) = (z \vee y) \wedge x$$

no es otra que (3) con x y z intercambiadas.

La proposición siguiente es inmediata:

Teorema 1. — *Todo subretículo de un retículo modular es modular.*

Teorema 2. — *El retículo de los subgrupos distinguidos de un grupo G es modular.*

Sean S_1, S_2, S_3 tres subgrupos distinguidos de G ; supongamos que $S_1 \subseteq S_3$. Tenemos

$$(S_1 \vee S_2) \wedge S_3 = S_1 S_2 \cap S_3.$$

Un elemento x perteneciente a este subgrupo es pues de la forma

$$x = s_1 s_2 = s_3, \quad \text{donde} \quad s_i \in S_i.$$

Tenemos

$$s_2 = s_1^{-1} s_3 \in S_3, \quad \text{puesto que} \quad S_1 \subseteq S_3,$$

luego

$$s_2 \in S_2 \cap S_3 \quad \text{y} \quad x \in S_1(S_2 \cap S_3) = S_1 \vee (S_2 \wedge S_3).$$

Hemos establecido así la inclusión

$$(S_1 \vee S_2) \wedge S_3 \leq S_1 \vee (S_2 \wedge S_3).$$

Como se tiene siempre, según (2), la inclusión en sentido contrario, de ello sigue la igualdad, esto es, la condición (3).

Corolarios. — 1. *El retículo de los subgrupos de un grupo abeliano es modular.*

2. Los retículos de los ideales a la izquierda, de los ideales a la derecha, de los ideales biláteros de un anillo A , son retículos modulares (según el corolario precedente y el teorema 1).

Observaciones. — 1. El retículo de los subgrupos distinguidos de un grupo G no es en general distributivo.

Consideremos, en efecto, el grupo abeliano libre G engendrado por dos elementos a, b , es decir, el conjunto de los elementos

$$a^m b^p = b^p a^m \quad (m, p \text{ enteros } \geq 0).$$

Sean S_1 el grupo monogéneo engendrado por a , S_2 el engendrado por b , S_3 el engendrado por $a b$. Tenemos:

$$S_1 \cap S_2 = (e), \quad (S_1 \wedge S_2) \vee S_3 = (e)S_3 = S_3.$$

Por otra parte,

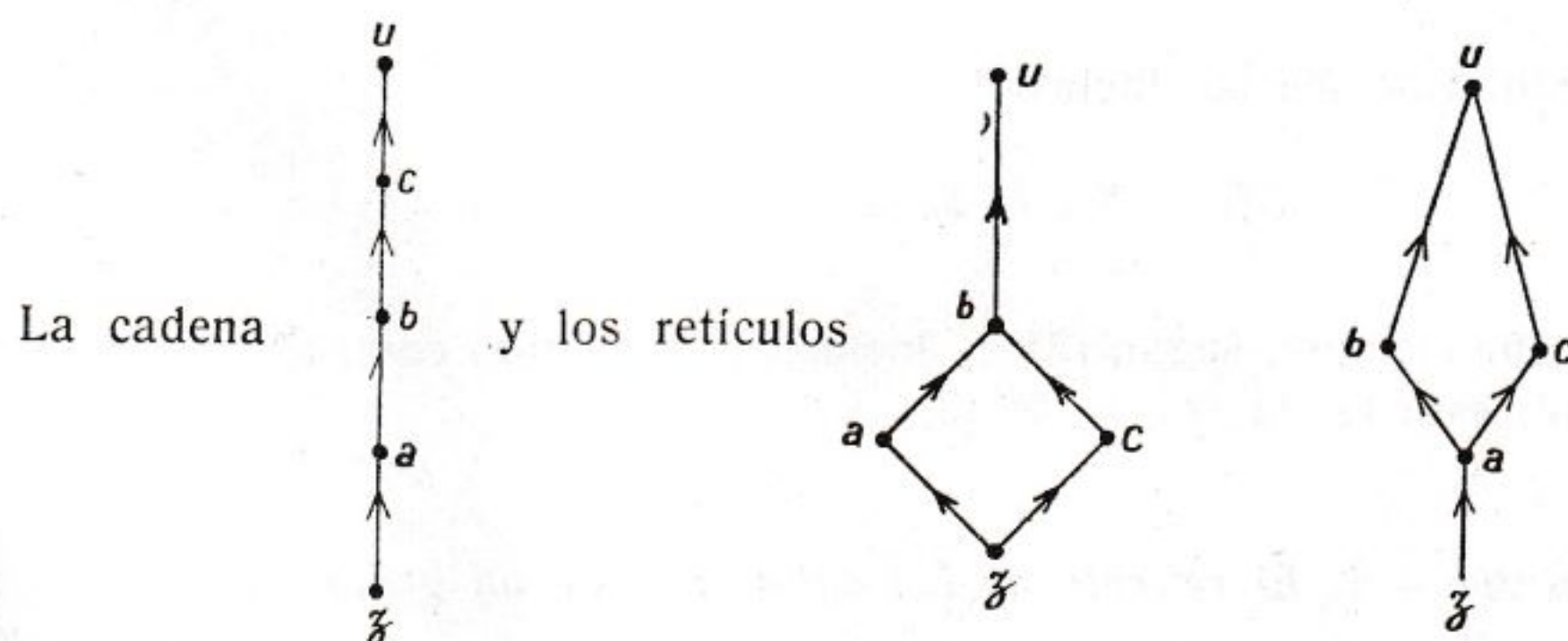
$$S_1 \vee S_3 = S_1 S_3 = G$$

pues $a^m b^p = a^{m-p} (ab)^p$. Del mismo modo $S_2 S_3 = G$, de donde

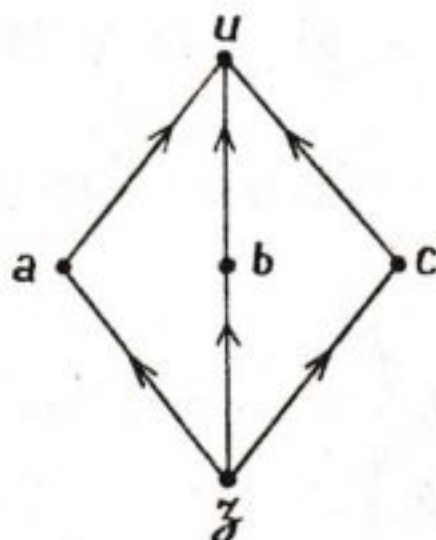
$$S_1 S_3 \wedge S_2 S_3 = G \wedge G = G \neq S_3.$$

2. En un anillo idempotente, luego conmutativo, con elemento unidad, el retículo de los ideales es distributivo, puesto que es el retículo de los filtros del retículo de Boole asociado.

Hemos visto que con cinco elementos z, a, b, c, u se pueden construir cuatro tipos de retículos con u como elemento universal y z como elemento nulo.

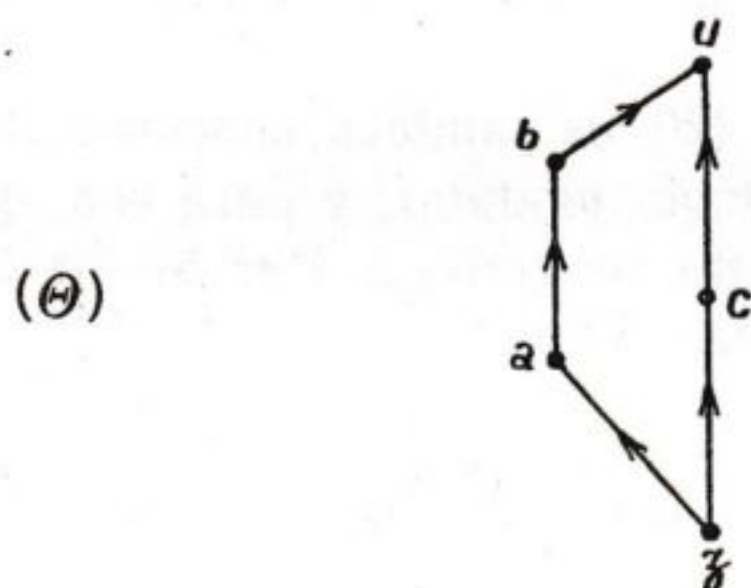


son distributivos, luego son modulares; como ya hemos visto, el retículo



no es distributivo, pero sí es modular.

Demostremos en fin que el retículo:



no es modular.

Tomemos $x = a$, $z = b$, $y = c$. El elemento

$$x \vee (y \wedge z) = a \vee (c \wedge b) = a \vee z = a$$

es distinto de

$$(x \vee y) \wedge z = (a \vee c) \wedge b = u \wedge b = b.$$

Puesto que todo subretículo de un retículo modular también lo es, *para que un retículo sea modular, es necesario que no contenga ningún subretículo de este tipo Θ.*

Consideremos ahora, en un retículo *modular*, tres elementos a, b, c ligados por las relaciones

$$\begin{aligned} a &\leq b \\ c \wedge a &= c \wedge b \\ c \vee a &= c \vee b. \end{aligned}$$

Tenemos

$$a = a \vee (c \wedge a) = a \vee (c \wedge b) = (a \vee c) \wedge b = (b \vee c) \wedge b = b.$$

Así, todo retículo modular verifica la condición siguiente:

$$B) \quad \left. \begin{array}{l} a \leq b \\ c \wedge a = c \wedge b \\ c \vee a = c \vee b \end{array} \right\} \text{ implican } a = b$$

en donde $a \leq b$ puede evidentemente sustituirse por: a y b son comparables.

Observemos, además, que esta nueva condición (B), condición necesaria para que un retículo sea modular, equivale a la *inexistencia de subretículos de cinco elementos del tipo Θ* .

Probemos que la condición (B) es también suficiente, lo que proporcionará una nueva definición de un retículo modular, y para eso, que, en un retículo $\mathfrak{C}$ no modular, la condición B no se verifica. Por hipótesis, existen en $\mathfrak{C}$ elementos x, y, z tal que se tenga, según (1),

$$x < z \quad \text{y} \quad x \vee (y \wedge z) < (x \vee y) \wedge z$$

siendo esta última desigualdad estricta. Consideremos entonces los elementos

$$\begin{aligned} a &= x \vee (y \wedge z), \\ b &= (x \vee y) \wedge z; \end{aligned}$$

tenemos

$$a < b \quad \text{estrictamente,}$$

y, cualquiera que sea $c \in \mathfrak{C}$,

$$\begin{aligned} a \vee c &\leq b \vee c, \\ a \wedge c &\leq b \wedge c. \end{aligned}$$

Tomemos entonces $c = y$; resulta:

$$\begin{aligned} a \vee c &= x \vee (y \wedge z) \vee y = x \vee y, \\ b \vee c &= [(x \vee y) \wedge z] \vee y \leq [(x \vee y) \wedge z] \vee (x \vee y) = x \vee y \end{aligned}$$

luego

$$b \vee c \leq a \vee c,$$

y por consiguiente

$$a \vee c = b \vee c.$$

Del mismo modo calculamos:

$$b \wedge c = (x \vee y) \wedge z \wedge y = y \wedge z,$$

$$a \wedge c = [x \vee (y \wedge z)] \wedge y \geq [x \vee (y \wedge z)] \wedge (y \wedge z) = y \wedge z$$

de donde

$$b \wedge c \leq a \wedge c$$

y por consiguiente

$$b \wedge c = a \wedge c.$$

Así, la condición (B) no se cumple, y podemos enunciar el teorema siguiente:

Teorema 3. — *Los retículos modulares son los retículos que verifican la condición*

$$B) \quad \left. \begin{array}{l} a \text{ y } b \text{ comparables} \\ a \wedge c = b \wedge c \\ a \vee c = b \vee c \end{array} \right\} \text{ implican } a = b.$$

Resulta entonces:

Teorema 4. — *Los retículos modulares son los retículos que no admiten ningún subretículo de cinco elementos del tipo (Θ) .*

El teorema 3 permite establecer una proposición análoga para los retículos distributivos. Como hemos visto en § 6, en todo retículo distributivo, las igualdades

$$a \wedge c = b \wedge c$$

$$a \vee c = b \vee c$$

implican $a = b$. Probemos que, recíprocamente, todo retículo $\mathfrak{C}$ en el cual vale esta propiedad, es distributivo.

La propiedad es válida, en particular, si a y b son comparables. Por consiguiente, el retículo $\mathfrak{C}$ es, al menos, modular. Sean x, y, z tres elementos cualesquiera de $\mathfrak{C}$; pongamos:

$$\begin{aligned} a &= (x \wedge y) \vee [z \wedge (x \vee y)], \\ b &= (y \wedge z) \vee [x \wedge (y \vee z)]. \end{aligned}$$

Puesto que $\mathfrak{C}$ es modular, la desigualdad $x \wedge y \leq x \vee y$ permite escribir

$$a = [(x \wedge y) \vee z] \wedge (x \vee y),$$

e igualmente tenemos

$$b = [(y \wedge z) \vee x] \wedge (y \vee z);$$

estas expresiones son duales de las precedentes. Tomemos $c = y$ tenemos

$$a \wedge c = [(x \wedge y) \vee z] \wedge y$$

de donde, utilizando la desigualdad $x \wedge y \leq y$ y la condición modular

$$a \wedge c = (x \wedge y) \vee (z \wedge y).$$

La expresión de $b \wedge c$ se obtiene permutando x y z :

$$b \wedge c = (z \wedge y) \vee (x \wedge y) = a \wedge c$$

Por dualidad, se tiene asimismo

$$b \vee c = a \vee c$$

luego

$$a = b$$

de donde

$$a \wedge x = b \wedge x.$$

Ahora bien

$$a \wedge x = \{[(x \wedge y) \vee z] \wedge (x \vee y)\} \wedge x = [(x \wedge y) \vee z] \wedge x.$$

de donde, utilizando la desigualdad $x \wedge y \leq x$ y la condición modular,

$$a \wedge x = (x \wedge y) \vee (z \wedge x).$$

Igualmente,

$$b \wedge x = \{(y \vee z) \wedge [x \vee (y \wedge z)]\} \wedge x = (y \vee z) \wedge x.$$

Tenemos pues finalmente

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

y el retículo $\mathfrak{C}$ es distributivo. Por consiguiente:

Teorema 5. — *Para que un retículo sea distributivo, es necesario y suficiente que satisfaga a la condición*

$$\left. \begin{array}{l} a \wedge c = b \wedge c \\ a \vee c = b \vee c \end{array} \right\} \text{ implican } a = b.$$

Probemos ahora que la condición (A) es equivalente a la inexistencia de subretículos de cinco elementos de los tipos Θ y M .

Hemos visto ya que la condición (A) implica esta inexistencia. Probemos ahora que, si (A) no es satisfecha, se puede encontrar en el retículo considerado un subretículo de uno de los tipos en cuestión.

Por hipótesis, existen en este retículo tres elementos a, b, c para los cuales no se verifica la condición (A). Si a y b son comparables, es inmediato, como hemos visto, que existe un subretículo del tipo Θ . Supongamos, pues, ahora que (A) sea falsa con elementos a, b no comparables. El retículo es entonces modular. Vamos a encontrar un subretículo del tipo M .

El subretículo engendrado por a, b, c , contiene, con estos tres elementos, los elementos

$$a \wedge c = b \wedge c = a \wedge b \wedge c = i$$

y

$$a \vee c = b \vee c = a \vee b \vee c = s,$$

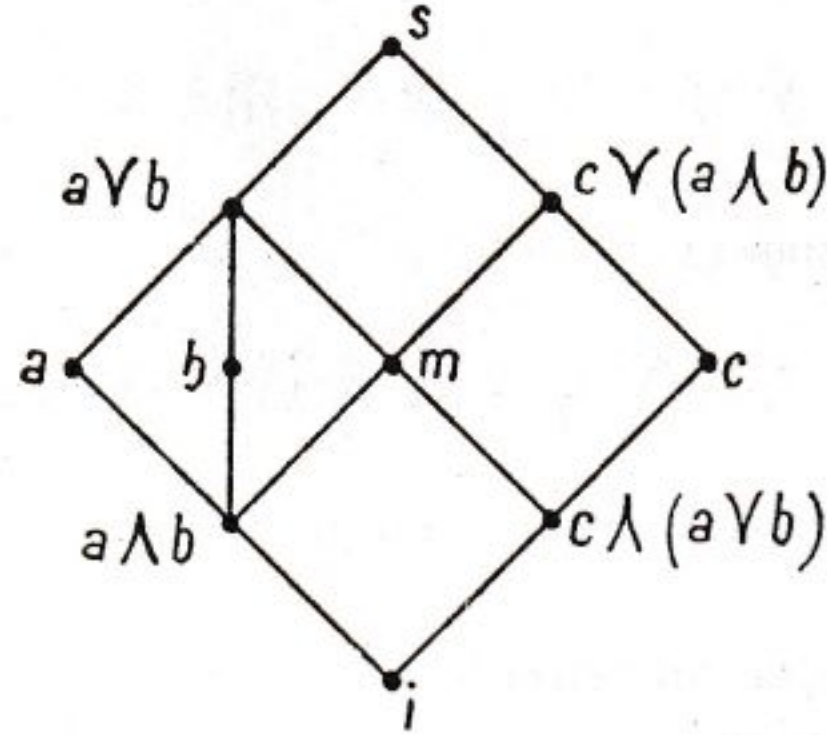
luego los elementos

$$c \wedge (a \vee b), \quad c \vee (a \wedge b)$$

y

$$(a \wedge b) \vee [c \wedge (a \vee b)] = m_1,$$

$$(a \vee b) \wedge [c \vee (a \wedge b)] = m_2.$$



Ahora bien, según la condición modular (aplicada teniendo en cuenta $a \wedge b \prec a \vee b$), tenemos:

$$(a \wedge b) \vee [c \wedge (a \vee b)] = [(a \wedge b) \vee c] \wedge (a \vee b)$$

Los dos elementos m_1 y m_2 son entonces iguales: designémosles por m . La igualdad $m = a$ implicaría $m = b$, por simetría, lo que es imposible puesto que tenemos por hipótesis $a \neq b$. En estas condiciones, probemos que los cinco elementos $a, b, m, z = a \wedge b, u = a \vee b$ forman un subretículo del tipo M , y por esto que

$$a \wedge m = a \wedge b (= b \wedge m \text{ por simetría}),$$

$$a \vee m = a \vee b (= b \vee m \text{ por simetría}).$$

Tenemos:

$$a \wedge m = a \wedge m_2 = a \wedge (a \vee b) \wedge [c \vee (a \wedge b)] = a \wedge [c \vee (a \wedge b)]$$

y, según la condición modular,

$$a \wedge m = (a \wedge b) \vee (a \wedge c) = a \wedge b.$$

Igualmente

$$a \vee m = a \vee m_1 = a \vee (a \wedge b) \vee [c \wedge (a \vee b)] = a \vee [c \wedge (a \vee b)]$$

$$= (a \vee c) \wedge (a \vee b) = a \vee b.$$

La proposición queda por tanto establecida.

Hemos obtenido así el:

Teorema 6. — *La condición (A) y la inexistencia de subretículos de los tipos Θ y M , son dos propiedades equivalentes.*

Resulta entonces:

Teorema 7. — *Para que un retículo sea distributivo, es necesario y suficiente que no contenga subretículos de los tipos Θ y M .*

Definición. — En un retículo que posea elemento mínimo z y elemento máximo u , una cadena finita, o sucesión estrictamente creciente, que vaya de z a u ,

$$\mathcal{A} \quad z = a_0 < a_1 < \dots < a_{k-1} < a_k = u$$

se llama *sucesión normal*; k , número de elementos menos uno, es la longitud de la cadena.

Una sucesión normal

$$\mathcal{B} \quad z = b_0 < b_1 < \dots < b_{l-1} < b_l = u$$

se llama *subdivisión* de $\mathcal{A}$ si es $\mathcal{A} \subseteq \mathcal{B}$, es decir, si para todo $a_j \in \mathcal{A}$, existe un $b_i \in \mathcal{B}$ tal que $b_i = a_j$.

Se llama *sucesión principal* a toda sucesión normal que sea maximal, es decir, que no admita más subdivisión que ella misma.

Teorema 8. — *En un retículo modular $\mathcal{C}$, dos sucesiones normales cualesquiera $\mathcal{A}$ y $\mathcal{B}$ admiten subdivisiones de la misma longitud.*

Consideremos el conjunto $\mathcal{A}^*$ de los elementos

$$a_{i,j} = a_i \vee (a_{i+1} \wedge b_j) \quad (i = 0, \dots, k-1; j = 0, \dots, l)$$

en número, a lo sumo, de $k(l+1)$; algunos de estos elementos pueden ser iguales. Probemos que $\mathcal{A}^*$ es una sucesión que contiene a $\mathcal{A}$.

Primeramente tenemos

$$a_{i,0} = a_i \vee (a_{i+1} \wedge z) = a_i = a_{i-1,l} = a_{i-1} \vee (a_i \wedge u)$$

$\mathcal{A}^*$ tiene pues a lo sumo kl elementos distintos y contiene a $\mathcal{A}$ como subconjunto.

Las relaciones

$$\begin{aligned} a_{i,j} &= a_i \vee (a_{i+1} \wedge b_j) \leq a_{i+1} \vee (a_{i+1} \wedge b_j) = a_{i+1} \\ a_r &\leq a_{r,s} = a_r \vee (a_{r+1} \wedge b_s) \end{aligned}$$

prueban que, para $i < r$, se tiene:

$$a_{i,j} \leq a_{r,s} \quad \text{cualesquiera sean } j, s \in \{1, \dots, l\}.$$

Como además $j < s$ implica $b_j < b_s$ y por consiguiente $a_{i,j} \leq a_{i,s}$, tenemos

$$a_{i,j} \leq a_{r,s} \quad \text{si} \quad \begin{cases} i < r \\ \text{o} \\ i = r \end{cases} \quad \text{y} \quad j < s.$$

Igualmente, el conjunto $\mathcal{B}^*$ de los elementos

$$b_{j,i} = b_j \vee (b_{j+1} \wedge a_i)$$

contiene a $\mathcal{B}$ y está totalmente ordenado.

No podemos afirmar que $\mathcal{A}^*, \mathcal{B}^*$ son sucesiones estrictamente crecientes, pero vamos a demostrar que el número de igualdades entre elementos consecutivos es el mismo en $\mathcal{A}^*$ que en $\mathcal{B}^*$ y para esto, por ejemplo, que

$$a_{i,j} = a_{i,j+1} \quad \text{implica} \quad b_{j,i} = b_{j,i+1}.$$

Tenemos

$$a_{i,j+1} = a_i \vee (a_{i+1} \wedge b_{j+1})$$

donde $a_i < a_{i+1}$; luego, por ser $\mathcal{G}$ modular,

$$a_{i,j+1} = (a_i \vee b_{j+1}) \wedge a_{i+1}$$

de donde

$$a_{i,j+1} \wedge b_{j+1} = a_{i+1} \wedge b_{j+1}.$$

La igualdad $a_{i,j} = a_{i,j+1}$ implica pues

$$a_{i+1} \wedge b_{j+1} = a_{i,j} \wedge b_{j+1} = [a_i \vee (a_{i+1} \wedge b_j)] \wedge b_{j+1},$$

donde $a_{i+1} \wedge b_j \leq b_j < b_{j+1}$ utilizando de nuevo la condición modular, se obtiene

$$a_{i+1} \wedge b_{j+1} = (a_{i+1} \wedge b_j) \vee (a_i \wedge b_{j+1}).$$

Teniendo esto, podemos escribir

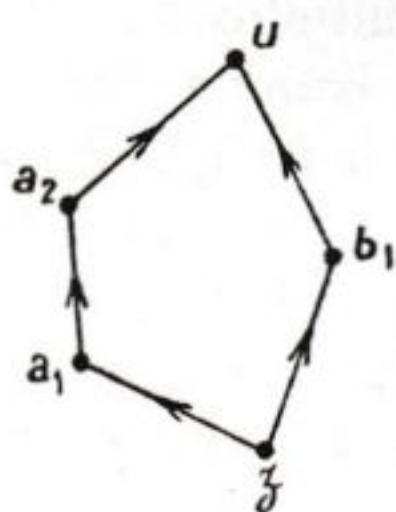
$$\begin{aligned} b_{j,i+1} &= b_j \vee (b_{j+1} \wedge a_{i+1}) \\ &= b_j \vee (a_{i+1} \wedge b_j) \vee (a_i \wedge b_{j+1}) \\ &= b_j \vee (b_{j+1} \wedge a_i) = b_{j,i} \end{aligned}$$

como era necesario demostrar.

Las cadenas $\mathcal{A}'$, $\mathcal{B}'$ formadas respectivamente por los elementos distintos de $\mathcal{A}^*$ y los elementos distintos de $\mathcal{B}^*$ tienen la misma longitud y el teorema 8 queda demostrado.

Si en particular $\mathcal{A}$ y $\mathcal{B}$ son sucesiones principales (es decir sucesiones finitas, estrictamente crecientes y maximales), se tiene $\mathcal{A}' = \mathcal{A}$, $\mathcal{B}' = \mathcal{B}$ y por consiguiente $\mathcal{A}$ y $\mathcal{B}$ tienen la misma longitud. Luego, si un retículo modular $\mathfrak{C}$ admite diversas sucesiones principales (finitas), todas ellas tienen la misma longitud.

Todo subretículo de $\mathfrak{C}$ tiene evidentemente la misma propiedad. Por otra parte, hemos visto que si un retículo no es modular, contiene un subretículo de la forma



que tiene una sucesión principal de longitud 2 y una sucesión principal de longitud 1. Por lo tanto, un retículo es modular si, y sólo si, en cualquier subretículo que tenga cadenas maximales (finitas), estas cadenas tienen la misma longitud.

Aplicación. — En el retículo de los subgrupos distinguidos de un grupo G , las sucesiones principales que van de un subgrupo dado a otro tienen todas la misma longitud.

Observación. — En el retículo de los subgrupos de G , que en general no es modular, se tienen propiedades más finas, que ulteriormente veremos.

§ 9. Conjuntos con una relación de orden y una ley de composición interna

Consideremos un conjunto E en el que estén dadas una relación de orden, que representaremos por el signo $\leq$ y una ley de composición interna que denotaremos multiplicativamente. Este tipo de estructura aparece frecuentemente, como muestran estos ejemplos: conjunto $\mathbf{N}$ de los enteros naturales (con el orden habitual y la multiplicación ordinaria, o con la adición); conjunto de las

partes de un conjunto con una ley de composición y la inclusión como relación de orden; conjunto de los subgrupos distinguidos de un grupo dado, también con la inclusión como relación de orden.

El estudio de los conjuntos E que tienen una multiplicación y una relación de orden se apoya sobre una hipótesis que exprese cierto concierto entre la ordenación y la operación dadas.

Definición. — Se dice que la multiplicación de E es *isótónica* (o *compatible* con la relación de orden) si

$$a \leq b \quad \text{implica} \quad ax \leq bx \quad \text{y} \quad xa \leq xb \quad \forall x \in E.$$

Si, desde el punto de vista multiplicativo, el conjunto E es un semigrupo o un grupo y su multiplicación es isótónica para esa relación de orden, se dirá que E es un *semigrupo ordenado* o un *grupo ordenado*.

Como conjunto ordenado, E puede tener propiedades más fuertes: ser un semirretículo o un retículo, lo que hace aparecer en E una o dos leyes de composición, $\vee$ (o sup), $\wedge$ (o inf); entonces cabe estudiar las propiedades que corresponden a unas tales leyes y a la multiplicación.

Teorema 1. — Sea E un conjunto ordenado y con una multiplicación isótónica; si E , para su relación de orden, es un inf-semirretículo se tiene

$$(1) \quad (a \wedge b)x \leq ax \wedge bx, \quad x(a \wedge b) \leq xa \wedge xb$$

cualesquiera que sean $a, b, x \in E$.

La desigualdad $a \wedge b \leq a$ implica en efecto $(a \wedge b)x \leq ax$; se tiene asimismo $(a \wedge b)x \leq bx$, y de aquí la primera desigualdad (1). La misma demostración vale para la segunda.

Se tiene un teorema análogo para un sup-semirretículo, que se traduce por las relaciones duales

$$(2) \quad ax \vee bx \leq (a \vee b)x, \quad xa \vee xb \leq x(a \vee b).$$

Es esencial observar que las desigualdades (1), por ejemplo, constituyen una propiedad más débil que la distributiva de la multiplicación respecto a la ley $\wedge$ y que la isotonía no implica esta distributividad. Hemos visto en efecto en el capítulo I (§ 4, 4.º) que en el conjunto $\mathcal{P}(M)$ de las partes de un conjunto M con una multiplicación, la multiplicación no es distributiva respecto a la intersección $\cap$; sin embargo lo es respecto a la unión $\cup$. Se llama *retículo multi-*

plicativo un retículo $\mathfrak{G}$ en el que existe una multiplicación distributiva con respecto a la ley $\vee$ (sup.) Por ejemplo, el conjunto $\mathfrak{I}(M)$, de partes de un conjunto M con una multiplicación, es un retículo multiplicativo. Los retículos $\mathfrak{I}_l, \mathfrak{I}_d, \mathfrak{I}$ de los ideales a la izquierda, a la derecha, biláteros de un anillo A son también retículos multiplicativos: el límite superior, $\vee$ es aquí la suma, que efectivamente está distribuida por la multiplicación (mientras que en general el límite inferior $\wedge$, intersección conjuntista $\cap$, no lo está).

Teorema 2. — *Si existe, en un $\vee$ -semirretículo $\mathfrak{G}$, una multiplicación distributiva respecto a la ley $\vee$, esta multiplicación es isótoma para la relación de orden de $\mathfrak{G}$.*

La relación de orden de $\mathfrak{G}$ está definida, a partir de la ley $\vee$, como se ha visto en § 5: la desigualdad $a \leq b$ significa $a \vee b = b$, lo que implica

$$x(a \vee b) = xb \quad \forall x \in \mathfrak{G}$$

es decir

$$xa \vee xb = xb \quad \text{o} \quad xa \leq xb.$$

Se obtiene de modo análogo $ax \leq bx$.

Se llama *grupo reticulado* un grupo (multiplicativo) G provisto de una relación de orden $\leq$ para la que es un retículo, cuyas operaciones $\wedge$ y $\vee$ son, además, distribuidas por la multiplicación.

De hecho, esta notable estructura se obtiene con hipótesis mucho menos fuertes.

Teorema 3. — *Todo grupo (multiplicativo) G con una relación de orden que verifica las dos condiciones siguientes:*

- a) *la multiplicación de G es isótoma,*
- b) *G es un $\vee$ -semirretículo,*

es un grupo reticulado. Además, G es un retículo distributivo.

Probemos primero que la multiplicación de G es distributiva respecto a la operación $\vee$. Como hemos visto más arriba, la isotonía implica

$$(2) \quad ax \vee bx \leq (a \vee b)x \quad \forall a, b, x \in G.$$

Recíprocamente, $ax \leq ax \vee bx$ implica $a \leq (ax \vee bx)x^{-1}$; se tiene asimismo $b \leq (ax \vee bx)x^{-1}$, de donde $a \vee b \leq (ax \vee bx)x^{-1}$ y finalmente

$$(a \vee b)x \leq ax \vee bx$$

que con (2) implica la igualdad, es decir la distributividad a la derecha. Se establece igualmente la distributividad a la izquierda.

Designemos por e el elemento unidad de G y observemos que por la isotonía, dos cualesquiera de las relaciones

$$\begin{aligned} x \leq y, & \quad xy^{-1} \leq e, & \quad y^{-1}x \leq e, \\ e \leq x^{-1}y, & \quad e \leq yx^{-1}, & \quad y^{-1} \leq x^{-1} \end{aligned}$$

son equivalentes,

La desigualdad $a \leq a \vee b$, escrita en la forma $(a \vee b)^{-1} \leq a^{-1}$, nos dice

$$a(a \vee b)^{-1}b \leq b.$$

Asimismo, $b \leq a \vee b$ o $(a \vee b)^{-1} \leq b^{-1}$, implica

$$a(a \vee b)^{-1}b \leq a.$$

Luego, el par (a, b) queda minorado por $a(a \vee b)^{-1}b$ y G es un conjunto filtrante inferiormente.

Si ahora x es un minorante del par a, b se tiene $a^{-1} \vee b^{-1} \leq x^{-1}$, es decir, a causa de la distributividad de la multiplicación con respecto a la unión,

$$b^{-1}(a \vee b)a^{-1} = a^{-1} \vee b^{-1} \leq x^{-1}$$

de donde

$$x \leq a(a \vee b)^{-1}b$$

El elemento $a(a \vee b)^{-1}b$ es, pues, el minorante máximo del par (a, b) , y G es un retículo, en el cual se tiene:

$$(3) \quad a \wedge b = a(a \vee b)^{-1}b$$

y asimismo (puesto que $\wedge$ es una ley conmutativa)

$$(3') \quad a \wedge b = b(a \vee b)^{-1}a.$$

Se tiene, según (3),

$$(4) \quad (a \wedge b)^{-1} = b^{-1}(a \vee b)a^{-1} = a^{-1} \vee b^{-1}.$$

Reemplazando en (4) a y b por sus inversos, y tomando luego los inversos de los dos miembros, obtenemos la fórmula dual

$$(4') \quad (a \vee b)^{-1} = a^{-1} \wedge b^{-1}$$

De (4) y (4') obtenemos

$$\begin{aligned} x(a \wedge b) &= x(a^{-1} \vee b^{-1})^{-1} = [(a^{-1} \vee b^{-1})x^{-1}]^{-1} \\ &= (a^{-1}x^{-1} \vee b^{-1}x^{-1})^{-1} = xa \wedge xb. \end{aligned}$$

La multiplicación es pues distributiva a la izquierda respecto a la ley $\wedge$; igualmente se establece la distributividad a la derecha.

Por último, si se tienen las dos igualdades

$$a \wedge c = b \wedge c$$

$$a \vee c = b \vee c$$

se puede escribir, según (3),

$$a \wedge c = a(a \vee c)^{-1}c$$

de donde

$$\begin{aligned} a &= (a \wedge c)c^{-1}(a \vee c) \\ &= (b \wedge c)c^{-1}(b \vee c) = b \end{aligned}$$

Resulta de ello que G es un retículo distributivo, lo que termina la demostración.

Ejemplo. — El conjunto G de las funciones reales definidas y continuas sobre el intervalo cerrado $S = [0,1]$ que toman en cada punto de él un valor estrictamente positivo, ordenado al poner

$$f \leq g \quad \text{si} \quad f(x) \leq g(x) \quad \forall x \in S$$

es un *retículo*; la función $f \vee g$ es la que en cada punto x de S tiene por valor $\sup [f(x), g(x)]$; $f \wedge g$ es la que en x vale $\inf [f(x), g(x)]$. Con la multiplicación habitual (Cap. I, § 4, 1.º) G es un grupo; basta ahora aplicar las reglas elementales del cálculo para constatar que G verifica las propiedades *a*) y *b*), e incluso las condiciones más fuertes del teorema 3: G es por lo tanto un grupo reticulado.

§ 10. Estudio del retículo multiplicativo de los ideales de un anillo conmutativo

Sea $\mathfrak{I}$ el retículo multiplicativo de los ideales de A (§ 9); en $\mathfrak{I}(A)$, $\mathfrak{I}$ es una familia de Moore, luego es un retículo completo, en el que el ínfimo es la intersección conjuntista $\cap$ y el supremo la suma Σ (cap. IV, § 7).

Consideremos en $\mathfrak{I}(A)$ la familia de Moore $\mathfrak{F}$ de las partes semiprimas para la multiplicación de A (cap. II, § 1, teor. 11); la intersección $\mathfrak{I} \cap \mathfrak{F} = \mathfrak{g}$ es también una familia de Moore en $\mathfrak{I}(A)$; sus elementos son, por definición, los *ideales semiprimos* de A (así, un ideal $\mathfrak{m}$ es semiprimo cuando todo elemento de A que tiene alguna de sus potencias en $\mathfrak{m}$, es, él mismo, elemento de $\mathfrak{m}$). Vamos a estudiar esta clase de ideales, y otros dos tipos que con ellos se relacionan: los ideales casi-primarios y los primarios.

El conjunto $\mathfrak{g}$ de los ideales semiprimos es también una familia de Moore en el retículo completo $\mathfrak{I}$ de los ideales de A . A esta familia está asociada, en $\mathfrak{I}$, una clausura de Moore $\mathfrak{m} \rightarrow \overline{\mathfrak{m}}$, donde $\overline{\mathfrak{m}}$ es el mínimo ideal semiprimo que contiene a $\mathfrak{m}$; por definición, $\overline{\mathfrak{m}}$ es el *radical* de $\mathfrak{m}$, y se le denota por $\mathcal{R}(\mathfrak{m})$. Tenemos inmediatamente las propiedades

$$\begin{aligned} \mathfrak{m} &\subseteq \mathcal{R}(\mathfrak{m}), \\ \mathfrak{m} \subseteq \mathfrak{m}' &\text{ implica } \mathcal{R}(\mathfrak{m}) \subseteq \mathcal{R}(\mathfrak{m}') \\ \mathcal{R}[\mathcal{R}(\mathfrak{m})] &= \mathcal{R}(\mathfrak{m}). \end{aligned}$$

Toda parte semiprima X que contiene a $\mathfrak{m}$ contiene necesariamente al conjunto S de los elementos s del anillo A que tienen alguna de sus potencias en $\mathfrak{m}$. Por ser S una parte semiprima, es la *mínima* parte semiprima que contiene a $\mathfrak{m}$.

Teorema 1. — *El conjunto S de los elementos s del anillo A que tienen alguna de sus potencias en $\mathfrak{m}$ coincide con el radical $\mathcal{R}(\mathfrak{m})$.*

Basta probar que S es un ideal. Puesto que A es conmutativo por hipótesis, es claro que

$$s \in S \quad \text{implica} \quad xs \in S \quad \forall x \in A.$$

Sean ahora a, b , dos elementos de S , y $a^\alpha \in \mathfrak{m}$, $b^\beta \in \mathfrak{m}$; será $(a - b)^\rho \in \mathfrak{m}$ siempre que cada uno de los productos $a^\lambda b^\mu$ con $\lambda + \mu = \rho$ pertenezca a $\mathfrak{m}$; ahora bien, esto es así para $\rho = \alpha + \beta - 1$ puesto que, entonces, o $\lambda \geq \alpha$

o $\mu \geq \beta$. Tenemos pues $a - b \in S$ luego S es un ideal.

El teorema 1 expresa que la clausura de Moore asociada a la familia $\mathfrak{g}$ de los ideales semiprimos, en $\mathfrak{J}$, no es otra cosa que la restricción a $\mathfrak{J}$ de la clausura en $\mathfrak{I}(A)$, asociada a la familia $\mathcal{F}$ de las partes semiprimas.

Teorema 2. — *Todo ideal primo $\mathfrak{p}$ es semiprimo: $\mathcal{R}(\mathfrak{p}) = \mathfrak{p}$.*

Basta demostrar que es $\mathcal{R}(\mathfrak{p}) \subseteq \mathfrak{p}$. Sea pues $x \in \mathcal{R}(\mathfrak{p})$ y sea α el mínimo entero natural para el que $x^\alpha \in \mathfrak{p}$. Si $\alpha = 1$, $x \in \mathfrak{p}$. Si $\alpha > 1$, las dos relaciones $x \cdot x^{\alpha-1} \in \mathfrak{p}$, $x^{\alpha-1} \notin \mathfrak{p}$ implican $x \in \mathfrak{p}$.

Observación. — El conjunto de los ideales primos, subconjunto del retículo $\mathfrak{g}$ de los ideales semiprimos, no es estable para la intersección. Consideremos en efecto, en un anillo conveniente A dos ideales primos $\mathfrak{p}_1, \mathfrak{p}_2$ no comparables por la inclusión y tales que se tenga $\mathfrak{p}_1 \cap \mathfrak{p}_2 \neq (0)$. Por ejemplo, designando $\mathbf{R}$ el cuerpo de los números reales, consideremos $A = \mathbf{R}[x, y, z]$ y $\mathfrak{p}_1 = (x, y)$, $\mathfrak{p}_2 = (x, z)$. Sean $p_1 \in \mathfrak{p}_1 - (\mathfrak{p}_1 \cap \mathfrak{p}_2)$, $p_2 \in \mathfrak{p}_2 - (\mathfrak{p}_1 \cap \mathfrak{p}_2)$; tenemos $p_1 p_2 \in \mathfrak{p}_1 \cap \mathfrak{p}_2$, mientras que ni p_1 , ni p_2 , pertenecen a esta intersección.

Teorema 3. — *Se tiene, para n ideales cualesquiera $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ del anillo A :*

$$\mathcal{R}(\mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n) = \mathcal{R}(\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n) = \mathcal{R}(\mathfrak{a}_1) \cap \dots \cap \mathcal{R}(\mathfrak{a}_n)$$

Las inclusiones

$$\mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n \subseteq \mathfrak{a}_i$$

implican

$$\mathcal{R}(\mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n) \subseteq \mathcal{R}(\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n) \subseteq \mathcal{R}(\mathfrak{a}_1) \cap \dots \cap \mathcal{R}(\mathfrak{a}_n).$$

Sea ahora $x \in \mathcal{R}(\mathfrak{a}_1) \cap \dots \cap \mathcal{R}(\mathfrak{a}_n)$; para cada índice i ($= 1, 2, \dots, n$), existe un entero positivo α_i tal que $x^{\alpha_i} \in \mathfrak{a}_i$, lo que tomando $\alpha = \alpha_1 + \dots + \alpha_n$, implica

$$x^\alpha \in \mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n, \quad \text{luego} \quad x \in \mathcal{R}(\mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n).$$

Tenemos pues

$$\mathcal{R}(\mathfrak{a}_1) \cap \dots \cap \mathcal{R}(\mathfrak{a}_n) \subseteq \mathcal{R}(\mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_n)$$

y, en consecuencia, vale la doble igualdad del enunciado

Corolario. — Se tiene : $\mathcal{R}(\mathfrak{a}^n) = \mathcal{R}(\mathfrak{a})$.

Observación. — Para una familia *infinita* de ideales $\mathcal{M}$, se tiene

$$\bigcap_{\mathfrak{m} \in \mathcal{M}} \mathfrak{m} \subseteq \mathfrak{m} \subseteq \mathcal{R}(\mathfrak{m})$$

y por consiguiente

$$\mathcal{R}\left(\bigcap_{\mathfrak{m} \in \mathcal{M}} \mathfrak{m}\right) \subseteq \bigcap_{\mathfrak{m} \in \mathcal{M}} \mathcal{R}(\mathfrak{m}),$$

pero la igualdad no vale en general. Tomemos, en efecto, el anillo de los enteros $\mathbf{Z}$ y consideremos la familia $\mathcal{M}$ de los ideales $\mathfrak{m}_n = (p^n)$, ($n = 1, 2, \dots$) donde p es un número primo fijo. Tenemos

$$\mathcal{R}(\mathfrak{m}_n) = (p) \quad \text{luego} \quad \bigcap_{\mathfrak{m} \in \mathcal{M}} \mathcal{R}(\mathfrak{m}) = (p)$$

Pero $\bigcap_{\mathfrak{m} \in \mathcal{M}} \mathfrak{m} = \bigcap_{n \in \mathbf{N}} (p^n) = (0)$, puesto que ningún entero no nulo es múltiplo

de todos los p^n ($n = 1, 2, \dots$). Tenemos, pues, aquí la inclusión estricta $(0) \subset (p)$.

Sea $\mathcal{E}$ la equivalencia asociada a la familia de los ideales semiprimos en el retículo de los ideales $\mathfrak{I}$; $\mathcal{E}$ está definida por

$$\mathfrak{a} \equiv \mathfrak{b}(\mathcal{E}) \quad \text{si} \quad \mathcal{R}(\mathfrak{a}) = \mathcal{R}(\mathfrak{b}).$$

Cualquiera que sea el ideal $\mathfrak{m} \in \mathfrak{I}$, tenemos

$$\begin{aligned} \mathcal{R}(\mathfrak{a}\mathfrak{m}) &= \mathcal{R}(\mathfrak{a} \cap \mathfrak{m}) = \mathcal{R}(\mathfrak{a}) \cap \mathcal{R}(\mathfrak{m}) = \mathcal{R}(\mathfrak{b}) \cap \mathcal{R}(\mathfrak{m}) = \mathcal{R}(\mathfrak{b} \cap \mathfrak{m}) \\ &= \mathcal{R}(\mathfrak{b}\mathfrak{m}) \end{aligned}$$

la equivalencia $\mathcal{E}$ es, pues, compatible con la multiplicación y la intersección de los ideales. Lo es también con la adición puesto que la suma se confunde con

el supremo $\bigvee$ en el retículo completo de los ideales (cf. § 4, corolario del teorema 2); la fórmula general se escribe, pues, aquí

$$\mathcal{R}\left(\sum_{\mathfrak{m} \in \mathcal{M}} \mathfrak{m}\right) = \mathcal{R}\left\{\sum_{\mathfrak{m} \in \mathcal{M}} [\mathcal{R}(\mathfrak{m})]\right\}$$

Definición. — En el anillo conmutativo A , se llama *ideal casi-primario* todo ideal $\mathfrak{q}$ cuyo radical es primo: $\mathcal{R}(\mathfrak{q}) = \mathfrak{p}$ (ideal primo).

Teorema 4. — Una condición necesaria y suficiente para que el ideal $\mathfrak{q}$ sea casi-primario es, que si el producto $ab \in \mathfrak{q}$, pero ninguna potencia de a pertenece a $\mathfrak{q}$, vaya implicado en ello que alguna potencia de b pertenece a $\mathfrak{q}$.

Supongamos $\mathfrak{q}$ casi-primario, $ab \in \mathfrak{q}$, $a^n \notin \mathfrak{q}$ ($\forall n = 1, 2, \dots$). Poniendo $\mathcal{R}(\mathfrak{q}) = \mathfrak{p}$, tenemos $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$, luego, siendo $\mathfrak{p}$ primo por hipótesis, $b \in \mathfrak{p}$ y existe una potencia b^β de b que pertenece a $\mathfrak{q}$.

Supongamos ahora que se cumple la condición del enunciado; sea $ab \in \mathcal{R}(\mathfrak{q})$, es decir $a^\lambda b^\lambda \in \mathfrak{q}$ ($\lambda \in \mathbf{N}$); una potencia de uno al menos de los dos elementos a^λ, b^λ pertenece a $\mathfrak{q}$ y por consiguiente uno al menos de los dos elementos a, b pertenece a $\mathcal{R}(\mathfrak{q})$; luego el ideal $\mathcal{R}(\mathfrak{q})$ es primo.

Vamos a ver que en un anillo conmutativo A con elemento unidad e , un ideal $\mathfrak{q}$ cuyo radical $\mathcal{R}(\mathfrak{q})$ es un ideal maximal $\mathfrak{m}$, tiene una propiedad más fuerte que la precedente. Supongamos, pues, que

$$ab \in \mathfrak{q} \quad \text{y} \quad \text{ninguna potencia de } a \text{ pertenece a } \mathfrak{q}.$$

Tenemos $a \notin \mathcal{R}(\mathfrak{q}) = \mathfrak{m}$, luego, puesto que $\mathfrak{m}$ es maximal,

$$\mathfrak{m} + (a) = A = (e),$$

y por consiguiente

$$e = m + ra \quad \text{con} \quad m \in \mathfrak{m}, r \in A.$$

Resulta de ello

$$b = mb + r \cdot ab \quad \text{es decir} \quad b \equiv mb \quad (\mathfrak{q})$$

de donde

$$b \equiv mb \equiv m^2b \equiv \dots \quad (\mathfrak{q})$$

Ahora bien, cierta potencia de m, m^μ , pertenece a $\mathfrak{q}$; tenemos pues

$$b \equiv m^\mu b \equiv 0 \quad (\mathfrak{q})$$

Así, el mismo b pertenece a $\mathfrak{q}$.

Definición. — Se llama *ideal primario* un ideal $\mathfrak{q}$ tal que las hipótesis

$$ab \in \mathfrak{q} \quad \text{y} \quad \text{ninguna potencia de } a \text{ pertenece a } \mathfrak{q}$$

impliquen $b \in \mathfrak{q}$.

Podemos enunciar:

Teorema 5. — En un anillo conmutativo A con elemento unidad, todo ideal cuyo radical es maximal es primario.

Todo ideal primario es casi-primario (entiéndase bien que esta propiedad, y la definición, son también válidas para un anillo sin elemento unidad).

Todo ideal primo $\mathfrak{p}$ es primario, y coincide con su radical.

Diremos que un ideal es *$\mathfrak{p}$ -primario* si es primario y admite el ideal primo $\mathfrak{p}$ como radical.

Teorema 6. — La intersección $\mathfrak{q} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ de un número finito de ideales $\mathfrak{q}_i$ que sean $\mathfrak{p}$ -primarios, es un ideal $\mathfrak{p}$ -primario.

Esta intersección tiene por radical $\mathfrak{p}$ (teorema 3) y por consiguiente es casi-primario. Mostremos que en efecto es primario. Sea $ab \in \mathfrak{q}$; supongamos que ninguna potencia de a pertenece a $\mathfrak{q}$, es decir $a \notin \mathfrak{p}$. Tenemos $ab \in \mathfrak{q}_i$ y ninguna potencia de a pertenece a $\mathfrak{q}_i$ ($i = 1, \dots, n$), luego

$$b \in \mathfrak{q}_i \quad (i = 1, \dots, n)$$

y por consiguiente $b \in \mathfrak{q}$.

Observación. — La propiedad no es cierta en general para una familia infinita Q de ideales $\mathfrak{p}$ -primarios $\mathfrak{q}$. Se ha visto por ejemplo que en el anillo $\mathbb{Z}$ de los enteros, si p designa un número primo la intersección de todos los ideales primarios (p^n) , de radical (p) , es el ideal primo (0) . Pero si existe un entero ρ tal que $\mathfrak{p}^\rho \subseteq \mathfrak{q}$ para todo ideal $\mathfrak{q}$ de la familia Q , se tiene, poniendo $\mathfrak{q}^* = \bigcap_{\mathfrak{q} \in Q} \mathfrak{q}$,

$\mathfrak{p}^\rho \subseteq \mathfrak{q}^*$. Si entonces $ab \in \mathfrak{q}^*$ y $a \notin \mathfrak{q}^*$, existe un ideal $\mathfrak{q}' \in Q$ tal que $a \notin \mathfrak{q}'$ y existe un entero λ tal que $b^\lambda \in \mathfrak{q}'$, de donde $b \in \mathfrak{p}$, $b^\rho \in \mathfrak{q}^*$, y por consiguiente $\mathfrak{q}^*$ es $\mathfrak{p}$ -primario.

Teorema 7. — *Para que un ideal $\mathfrak{q}$ sea casi-primario, es necesario y suficiente que el anillo $A/\mathfrak{q}$ de las clases residuales tenga la propiedad siguiente:*

I. *En $A/\mathfrak{q}$, todo divisor de cero es nilpotente o tiene sus anuladores nilpotentes.*

Para que un ideal $\mathfrak{q}$ sea primario, es necesario y suficiente que el anillo $A/\mathfrak{q}$ tenga la propiedad siguiente:

II. *En $A/\mathfrak{q}$, todo divisor de cero es nilpotente.*

a) Designemos por $\bar{0} (= \mathfrak{q})$ el elemento cero de $A/\mathfrak{q}$ y sean X, Y dos clases divisores de cero ($XY = \bar{0}$, $X \neq \bar{0}$, $Y \neq \bar{0}$). Sean x, y dos elementos de A que pertenecen respectivamente a las clases X, Y ; tenemos $xy \in \mathfrak{q}$. Supongamos X no nilpotente: $X^\alpha \neq \bar{0}$, $x^\alpha \notin \mathfrak{q}$ cualquiera que sea $\alpha = 1, 2, \dots$. Si $\mathfrak{q}$ es *casi-primario*, existe un entero β tal que $y^\beta \in \mathfrak{q}$, de donde $Y^\beta = \bar{0}$: Y , anulador de X , es nilpotente, lo que establece la propiedad I. Si $\mathfrak{q}$ es *primario*, se tiene $y \in \mathfrak{q}$, $Y = \bar{0}$, contrariamente a la hipótesis: X es necesariamente nilpotente, e igualmente Y , lo que establece la propiedad II.

b) Sean x, y dos elementos de A tales que se tenga $xy \in \mathfrak{q}$, $x^\alpha \notin \mathfrak{q}$ cualquiera que sea $\alpha = 1, 2, \dots$. Tenemos, si X, Y designan las clases módulo $\mathfrak{q}$ que contienen respectivamente a x, y , $XY = \bar{0}$, $X^\alpha \neq \bar{0}$ ($\alpha = 1, 2, \dots$).

Si $Y = \bar{0}$, $y \in \mathfrak{q}$; si no, X es divisor de cero no nilpotente; la propiedad I implica entonces que su anulador Y es nilpotente: $Y^\beta = \bar{0}$, $y^\beta \in \mathfrak{q}$, y $\mathfrak{q}$ es *casi-primario*; en cuanto a la propiedad II, implica que X no puede ser divisor de cero no nilpotente; se tiene, pues, necesariamente $y \in \mathfrak{q}$, y $\mathfrak{q}$ es *primario*.

Ejemplos. — 1. En el anillo $\mathbf{R}$ de los enteros, todo ideal de la forma (p^n) , donde p es primo, es un ideal $\mathfrak{p}$ -primario, siendo $\mathfrak{p}$ el ideal primo (p) ; en el anillo $\mathbf{R}[x, y]$, el ideal (x^2, y) es $\mathfrak{p}$ -primario, siendo $\mathfrak{p}$ el ideal (x, y) .

2. En el anillo $\mathbf{R}[x, y, z]$, el ideal

$$(x, y) \cap (x, y, z)^2 = (x^2, xy, y^2, xz, yz),$$

conjunto de los polinomios que, igualados a cero, definen las superficies que pasan por Oz y admiten O como punto doble al menos, es un ideal casi-primario, de radical $\mathfrak{p} = (x, y)$.

Definición. — Se llama *ideal primario fuerte* en el anillo conmutativo A un ideal $\mathfrak{q}$ tal que si dos ideales $\mathfrak{a}, \mathfrak{b}$ de A verifican $\mathfrak{ab} \subseteq \mathfrak{q}$, $\mathfrak{a} \not\subseteq \mathfrak{q}$, una potencia de $\mathfrak{b}$ esté contenida en $\mathfrak{q}$.

Teorema 8. — *Todo ideal primario fuerte $\mathfrak{q}$ es primario.*

Sean a, b dos elementos del anillo A verificando $ab \in \mathfrak{q}$, $a \notin \mathfrak{q}$. Consideremos los ideales principales engendrados por a y b : $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$. Tenemos $\mathfrak{a}\mathfrak{b} = (ab) \subseteq \mathfrak{q}$ y $\mathfrak{a} \not\subseteq \mathfrak{q}$, de donde, para un entero conveniente β , $\mathfrak{b}^\beta \subseteq \mathfrak{q}$ y por consiguiente $b^\beta \in \mathfrak{q}$.

§ 11. Residuación. Aplicación al estudio de las intersecciones de ideales primarios

Dado un conjunto E con una ley de composición interna conmutativa T , consideramos el conjunto $\mathfrak{F}(E)$ con la ley correspondiente, designada igualmente por T , y hemos visto que dados $A \in \mathfrak{F}(E)$ y $B \in \mathfrak{F}(E)$, no existe en general un elemento $C \in \mathfrak{F}(E)$ tal que $A \mathsf{T} C = B$.

$\mathfrak{F}(E)$ es aquí un conjunto con una ley de composición interna y con una relación de orden. Estas circunstancias nos van a permitir definir en $\mathfrak{F}(E)$, no la operación inversa de T , como cuando se tiene un grupo, sino una operación inversa aproximada, análoga a la división entera definida en el conjunto de los enteros, que da para resultado de $a : b$ el mayor entero c tal que ac sea menor o igual a b .

Consideremos, pues, el conjunto C de los elementos c de E tales que $A \mathsf{T} c \subseteq B$. Se tiene $A \mathsf{T} C \subseteq B$ y C es el mayor complejo de E tal que esta relación tenga lugar: C se denomina *residual* de B por A , y se indica por $C = B:A$.

Más generalmente, en el conjunto E con una ley de composición conmutativa T y con una relación de orden $\leq$ si para dos elementos a, b cualesquiera de E , el conjunto de los elementos c tales que $a \mathsf{T} c \leq b$ no es vacío y admite un elemento máximo c , se podrá llamar a éste el *residual* de b por a , $c = b : a$. En esta hipótesis, se define así, en E , la ley de composición asociada a T :

$$(1) \quad c = b : a \quad \Leftrightarrow \quad a \mathsf{T} c \leq b \quad \text{y} \quad a \mathsf{T} c' \leq b \quad \Rightarrow \quad c' \leq c$$

En particular, para un retículo multiplicativo $\mathfrak{G}$ vale lo que acabamos de decir: el *retículo* $\mathfrak{G}$ se llamará *residuado* si para todo par a, b de elementos de $\mathfrak{G}$ existe un c que satisface a las condiciones (1).

En particular, como acabamos de mostrar, el retículo $\mathfrak{F}(E)$ para la ley de composición T asociada a la de E es un retículo residuado. Tomemos como E un anillo conmutativo $\mathcal{A}$ y fijemos nuestra atención en la multiplicación del

anillo como operación T . . Estableceremos esta propiedad: *los ideales de $\mathcal{A}$ forman un subconjunto de $\mathfrak{I}(\mathcal{A})$ estable para la operación residuación en $\mathfrak{I}(\mathcal{A})$.*

Nos hace falta demostrar que:

$$C = \{c; c \in \mathcal{A}; cA \subseteq B\}$$

es un ideal cuando A y B son ideales. Vamos incluso a demostrar que C es un ideal cuando se supone solamente que lo es B . Esto resulta inmediatamente de que: 1.º $c_1A \subseteq B$ y $c_2A \subseteq B$ implican

$$(c_1 - c_2)A \subseteq B$$

(puesto que siendo B un subgrupo aditivo de $\mathcal{A}$, $c_1a \in B$ y $c_2a \in B$ implican $c_1a - c_2a \in B$), luego C es un subgrupo aditivo de $\mathcal{A}$. 2.º Si $cA \subseteq B$ para todo elemento ρ del anillo se tiene $cA\rho \subseteq B$, puesto que B es un ideal; luego, puesto que el anillo es conmutativo, $c \in C$ implica para todo $\rho (\in \mathcal{A})$ $c\rho \in C$.

Además:

La residuación de ideales en $\mathfrak{I}(\mathcal{A})$, definida a partir de la multiplicación de partes de $\mathcal{A}$, coincide con la residuación en el retículo $\mathfrak{C}$ de los ideales de $\mathcal{A}$, definida a partir de la multiplicación de ideales.

En efecto, se ha definido el producto de los ideales A y C , notado $A \div C$ como la clausura de Moore de $A \cdot C$ en el retículo de los ideales. Pero $AC \subseteq B$ implica $A \div C \subseteq B$ (isotonía e idempotencia de la clausura de Moore) y como inversamente $A \div D \subseteq B$, donde D es un ideal, implica $AD \subseteq B$, es decir $D \subseteq C$, C es también el máximo ideal tal que el ideal $A \div C$ esté contenido en B , luego *el retículo de los ideales es un retículo residuado.*

Propiedades del retículo de los ideales de un anillo conmutativo ligadas a la residuación. — 1.º $A : A = \mathcal{A}$; $A : (0) = \mathcal{A}$; $A \subseteq A : B, \forall B$; $B \subseteq A$ implica $A : B = \mathcal{A}$.

Estas propiedades resultan trivialmente de las propiedades de los ideales y de la definición del residual.

2.º Las propiedades siguientes resultan inmediatamente de la isotonía de la multiplicación en un retículo multiplicativo y son en particular ciertas en el retículo de los ideales:

$$\begin{array}{ll} A \subseteq A' & \text{implica} \quad A : B \subseteq A' : B \text{ (isotonía de la residuación)} \\ B' \subseteq B & \text{implica} \quad A : B \subseteq A : B' \end{array}$$

3.º $(A : B) : B'$ es por definición el máximo ideal C tal que $C \div B'$ esté

contenido en $A : B$, luego tal que $(B' \div C) \div B$ esté contenido en A . Pero el producto de ideales es asociativo y conmutativo. Se tiene pues

$$(B' \div C) \div B = (B' \div B) \div C$$

y C es el máximo ideal tal que $(B' \div B) \div C$ esté contenido en A . Se tiene, pues

$$(A : B) : B' = A : (B' \div B)$$

y por lo tanto

$$(A : B) : B' = (A : B') : B$$

Teorema 1. — *La intersección de ideales es distributiva respecto a la residuación.*

Sea $\mathfrak{J}$ una familia de ideales A . Sea

$$C = \left(\bigcap_{A \in \mathfrak{J}} A \right) : B,$$

C es, pues, el conjunto de los elementos c tales que $cB \subseteq A$ para todo A de la familia $\mathfrak{J}$. Se tiene, pues, $C \subseteq A : B, \forall A \in \mathfrak{J}$ y, por lo tanto

$$\left(\bigcap_{A \in \mathfrak{J}} A \right) : B \subseteq \bigcap_{A \in \mathfrak{J}} (A : B).$$

Pero, inversamente, sea

$$c \in \bigcap_{A \in \mathfrak{J}} (A : B);$$

se tiene $c \in A : B$ para $A \in \mathfrak{J}$, luego

$$cB \in \bigcap_{A \in \mathfrak{J}} A \quad \text{y} \quad c \in \left(\bigcap_{A \in \mathfrak{J}} A \right) : B,$$

es decir

$$\bigcap_{A \in \mathfrak{J}} (A : B) \subseteq \left(\bigcap_{A \in \mathfrak{J}} A \right) : B$$

de donde la propiedad enunciada:

$$\left(\bigcap_{A \in \mathfrak{J}} A \right) : B = \bigcap_{A \in \mathfrak{J}} (A : B),$$

Teorema 2. — Si $\mathfrak{J}$ es una familia de ideales A e indicamos por $\bigvee_{A \in \mathfrak{J}} A = \sum_{A \in \mathfrak{J}} A$ al ideal $\sup (A)$ para $A \in \mathfrak{J}$, se tiene la relación

$$B : \left(\bigvee_{A \in \mathfrak{J}} A \right) = \bigcap_{A \in \mathfrak{J}} (B : A)$$

En efecto

$$A \subseteq \bigvee_{A \in \mathfrak{J}} A$$

implica desde luego

$$B : \left(\bigvee_{A \in \mathfrak{J}} A \right) \subseteq B : A$$

para todo A de la familia, luego

$$B : \left(\bigvee_{A \in \mathfrak{J}} A \right) \subseteq \bigcap_{A \in \mathfrak{J}} (B : A)$$

Por otra parte, $cA \subseteq B$ para $\forall A \in \mathfrak{J}$ implica asimismo $\sum_{A \in \mathfrak{J}} cA \subseteq B$ es decir

$$c \cdot \sum_{A \in \mathfrak{J}} A = c \cdot \left(\bigvee_{A \in \mathfrak{J}} A \right) \subseteq B$$

de donde

$$\bigcap_{A \in \mathfrak{J}} (B : A) \subseteq B : \left(\bigvee_{A \in \mathfrak{J}} A \right)$$

que termina la demostración.

Teorema 3. — Si $\mathfrak{q}$ es un ideal primario, el ideal $\mathfrak{q} : \mathfrak{a}$ es también primario, para cualquier ideal $\mathfrak{a}$.

1.º Si $\mathfrak{a} \subseteq \mathfrak{q}$, se tiene $\mathfrak{q} : \mathfrak{a} = \mathcal{A}$ y el anillo completo es primario.

2.º Si $\mathfrak{a} \not\subseteq \mathcal{R}(\mathfrak{q})$ (designamos siempre con $\mathcal{R}(\mathfrak{q})$ al radical de $\mathfrak{q}$), se puede elegir un $a \in \mathfrak{a}$, con $a \notin \mathcal{R}(\mathfrak{q})$. Sea entonces x un elemento cualquiera de $\mathfrak{q} : \mathfrak{a}$. Se tiene $ax \in \mathfrak{q}$ y como $\mathfrak{q}$ es primario y $a \notin \mathcal{R}(\mathfrak{q})$, es $x \in \mathfrak{q}$. Se tiene pues $\mathfrak{q} : \mathfrak{a} \subseteq \mathfrak{q}$. Pero se tiene siempre

$$\mathfrak{q} \subseteq \mathfrak{q} : \mathfrak{a}.$$

luego

$$\mathfrak{a} \not\subseteq \mathcal{R}(\mathfrak{q}) \quad \text{implica} \quad \mathfrak{q} = \mathfrak{q} : \mathfrak{a}$$

de donde resulta efectivamente que $\mathfrak{q} : \mathfrak{a}$ es primario.

3.º Si $\mathfrak{a} \subseteq \mathcal{R}(\mathfrak{q})$, sean $xy \in \mathfrak{q} : \mathfrak{a}$ y ninguna potencia de y esté en $\mathfrak{q} : \mathfrak{a}$. Sea $a \in \mathfrak{a}$; tenemos la relación $axy \in \mathfrak{q}$. Ninguna potencia de y pertenece a $\mathfrak{q}$ por la imposibilidad de que $y^s \in \mathfrak{q} \subseteq \mathfrak{q} : \mathfrak{a}$. Se tiene pues, ya que $\mathfrak{q}$ es primario, $ax \in \mathfrak{q}$, y esto es así para todo $a \in \mathfrak{a}$. Con esto resulta que $x \in \mathfrak{q} : \mathfrak{a}$ y queda demostrado que $\mathfrak{q} : \mathfrak{a}$ es primario.

Se tiene además:

Teorema 4. — Si $\mathfrak{a} \subseteq \mathcal{R}(\mathfrak{q})$, $\mathfrak{a} \not\subseteq \mathfrak{q}$, el ideal primario $\mathfrak{q} : \mathfrak{a}$ tiene igual radical que $\mathfrak{q}$.

La desigualdad $\mathfrak{q} \subseteq \mathfrak{q} : \mathfrak{a}$ implica ya $\mathcal{R}(\mathfrak{q}) \subseteq \mathcal{R}(\mathfrak{q} : \mathfrak{a})$. Pero si $x \in \mathcal{R}(\mathfrak{q} : \mathfrak{a})$ existe un entero s tal que $x^s \in (\mathfrak{q} : \mathfrak{a})$. Se tiene pues $x^s \mathfrak{a} \subseteq \mathfrak{q}$. Pero $\mathfrak{a} \not\subseteq \mathfrak{q}$ implica la existencia de $a \in \mathfrak{a}$, $a \notin \mathfrak{q}$, y se tiene $x^s a \in \mathfrak{q}$; $a \notin \mathfrak{q}$; por ser $\mathfrak{q}$ primario, existe un entero t tal que $(x^s)^t = x^{st} \in \mathfrak{q}$ y $x \in \mathcal{R}(\mathfrak{q})$, lo que era necesario demostrar.

Corolario. — Si $\mathfrak{p}$ es primo, y si $\mathfrak{a} \subset \mathfrak{p}$, se tiene $\mathfrak{p} : \mathfrak{a} = \mathcal{A}$. Si $\mathfrak{a} \not\subseteq \mathfrak{p}$ se tiene $\mathfrak{p} : \mathfrak{a} = \mathfrak{p}$, y sólo estos dos casos son posibles.

Demos como aplicación de la residuación algunas propiedades de la intersección de un número finito de ideales primarios de radicales diferentes y sin elemento superfluo en un anillo conmutativo $\mathcal{A}$; intersecciones que llamamos *normadas*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_r$$

1.º Si $\mathfrak{a}$ es primario, se tiene $r = 1$.

Pongamos, en efecto,

$$\mathfrak{m} = \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_r.$$

Se tiene:

$$\mathfrak{a} : \mathfrak{m} = (\mathfrak{q}_1 \cap \mathfrak{m}) : \mathfrak{m}$$

de donde, según el teorema 1:

$$\mathfrak{a} : \mathfrak{m} = (\mathfrak{q}_1 : \mathfrak{m}) \cap (\mathfrak{m} : \mathfrak{m}) = (\mathfrak{q}_1 : \mathfrak{m}) \cap \mathcal{A} = \mathfrak{q}_1 : \mathfrak{m}$$

Pero es $\mathfrak{m} \not\subseteq \mathfrak{q}_1$, puesto que $\mathfrak{m} \subseteq \mathfrak{q}_1$ implicaría que $\mathfrak{q}_1$ fuese superfluo. Como $\mathfrak{a} \subseteq \mathfrak{q}_1$, se tiene también $\mathfrak{m} \not\subseteq \mathfrak{a}$. En virtud del teorema 3, $\mathfrak{a} : \mathfrak{m}$ es primario de radical $\mathcal{R}(\mathfrak{a})$, $\mathfrak{q}_1 : \mathfrak{m}$ es primario de radical $\mathcal{R}(\mathfrak{q}_1)$. Se tiene pues

$$\mathcal{R}(\mathfrak{q}_1) = \mathcal{R}(\mathfrak{a})$$

y de la misma manera

$$\mathcal{R}(\mathfrak{q}_i) = \mathcal{R}(\mathfrak{a})$$

para $i = 1, \dots, r$. Para obtener una intersección normada, debemos reemplazar todos los ideales primarios de igual radical por su intersección, teniendo en este caso, necesariamente, $r = 1$.

2.º La igualdad

$$\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_r = \mathfrak{q}'_1 \cap \dots \cap \mathfrak{q}'_s$$

entre intersecciones normadas de ideales primarios implica $r = s$ y, con índices convenientemente ordenados $\mathcal{R}(\mathfrak{q}_i) = \mathcal{R}(\mathfrak{q}'_i)$, $i = 1, \dots, r$.

Hemos visto que la propiedad es cierta para $r = 1$, y ahora procederemos por inducción sobre r . Supongamos, con la oportuna elección de índices, que $\mathcal{R}(\mathfrak{q}_r)$ sea maximal en el conjunto de los $\mathcal{R}(\mathfrak{q}_j)$ y $\mathcal{R}(\mathfrak{q}'_i)$. Existe un $\mathfrak{q}'_s$ tal que $\mathcal{R}(\mathfrak{q}'_s) = \mathcal{R}(\mathfrak{q}_r)$, pues de lo contrario se tendría

$$\mathfrak{q}_r \not\subseteq \mathcal{R}(\mathfrak{q}_j), j = 1, 2, \dots, r-1; \quad \mathfrak{q}_r \not\subseteq \mathcal{R}(\mathfrak{q}'_i), i = 1, 2, \dots, s$$

ya que la inclusión implicaría la de $\mathcal{R}(\mathfrak{q}_r)$ supuesto maximal para $\mathcal{R}(\mathfrak{q}_j)$ y $\mathcal{R}(\mathfrak{q}'_i)$. La igualdad

$$\left(\bigcap_{i=1}^r \mathfrak{q}_i \right) : \mathfrak{q}_r = \left(\bigcap_{j=1}^s \mathfrak{q}'_j \right) : \mathfrak{q}_r$$

se escribe

$$\bigcap_{i=1}^r \mathfrak{q}_i : \mathfrak{q}_r = \bigcap_{j=1}^s \mathfrak{q}'_j : \mathfrak{q}_r$$

y, por el teorema 3,

$$\mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_{r-1} \cap \mathcal{A} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_{r-1} = \mathfrak{q}'_1 \cap \mathfrak{q}'_2 \dots \cap \mathfrak{q}'_s$$

y $\mathfrak{q}_r$ sería superfluo.

Sea, pues,

$$\mathcal{R}(\mathfrak{q}'_s) = \mathcal{R}(\mathfrak{q}_r).$$

Pongamos $\mathfrak{q}_r^* = \mathfrak{q}_r \cap \mathfrak{q}'_s$ se sabe que $\mathfrak{q}'_r$ es primario de radical $\mathcal{R}(\mathfrak{q}_r)$ y $\mathfrak{q}_r^*$ está contenido en $\mathfrak{q}'_s$.

Se tiene la igualdad

$$\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_{r-1} \cap \mathfrak{q}_r^* = \mathfrak{q}'_1 \cap \dots \cap \mathfrak{q}'_{s-1} \cap \mathfrak{q}_r^*.$$

Residuando los dos miembros de esta igualdad por $\mathfrak{q}_r^*$, el mismo cálculo anterior nos da

$$\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_{r-1} = \mathfrak{q}'_1 \cap \dots \cap \mathfrak{q}'_{s-1}$$

y por la hipótesis de recurrencia $r - 1 = s - 1$, luego $r = s$, y

$$\mathcal{R}(\mathfrak{q}_i) = \mathcal{R}(\mathfrak{q}'_i), \quad i = 1, 2, \dots, r - 1$$

que junto con

$$\mathcal{R}(\mathfrak{q}_r) = \mathcal{R}(\mathfrak{q}'_r),$$

demuestra la propiedad. Se puede enunciar:

Teorema 5. — *Considerando en un anillo conmutativo dos intersecciones finitas de ideales primarios normadas (es decir, tales que los ideales que figuran en cada intersección tengan radicales diferentes y que ninguno sea superfluo en la intersección), si ambas son iguales tienen el mismo número de componentes; y los radicales de los componentes de ambas intersecciones son los mismos.*

Un razonamiento del mismo género nos va a permitir completar ese teorema de unicidad.

Definición. — Llamaremos *componente aislado* de la intersección

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_r,$$

a toda intersección parcial de ideales primarios $\mathfrak{q}_i$ tales que sus radicales no incluyan a ninguno de los radicales de los otros ideales primarios. Con una oportuna elección de índices, sea

$$\mathfrak{b} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_h$$

un componente aislado; entonces $\mathfrak{p}_i$, $i = 1, \dots, h$, no contiene a ningún $\mathfrak{p}_j$, $j = h+1, \dots, r$. Sean entonces $\mathfrak{q}'_1 \cap \dots \cap \mathfrak{q}'_r$ otra representación de $\mathfrak{a}$, y $\mathfrak{b}' = \mathfrak{q}'_1 \cap \dots \cap \mathfrak{q}'_h$ un componente aislado de ella con el mismo radical que $\mathfrak{b}$. Vamos a demostrar que $\mathfrak{b} = \mathfrak{b}'$. Pondremos

$$\mathfrak{I} = \mathfrak{q}_{h+1} \cap \dots \cap \mathfrak{q}_r, \quad \mathfrak{I}' = \mathfrak{q}'_{h+1} \cap \dots \cap \mathfrak{q}'_r.$$

Se tiene, primeramente

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{I} = \mathfrak{b}' \cap \mathfrak{I}' \quad \text{y} \quad \mathfrak{I} \not\subseteq \mathfrak{p}_i, i = 1, \dots, h$$

(y lo mismo para $\mathfrak{I}'$). En efecto, $\mathfrak{I} \subseteq \mathfrak{p}_i$ implicaría

$$\mathcal{R}(\mathfrak{I}) = \mathfrak{p}_{h+1} \cap \dots \cap \mathfrak{p}_r \subseteq \mathfrak{p}_i, \quad \text{de donde} \quad \mathfrak{p}_{h+1} \dots \mathfrak{p}_r \subseteq \mathfrak{p}_i$$

y, como $\mathfrak{p}_i$ es primo, resultaría que alguno de los ideales

$$\mathfrak{p}_j \quad (j = h+1, \dots, r)$$

estaría contenido en $\mathfrak{p}_i$, contra la hipótesis. Pero entonces tenemos

$$\mathfrak{b} : \mathfrak{I} = \bigcap_{i=1}^h \mathfrak{q}_i : \mathfrak{I} = \bigcap_{i=1}^h \mathfrak{q}_i = \mathfrak{b}$$

y

$$\mathfrak{a} : \mathfrak{I} = (\mathfrak{b} : \mathfrak{I}) \cap \mathfrak{I} : \mathfrak{I} = \mathfrak{b} \cap \mathcal{A} = \mathfrak{b}$$

Mas como también se tiene

$$\mathfrak{a} = \mathfrak{b}' \cap \mathfrak{I}',$$

resulta

$$\mathfrak{a} : \mathfrak{I} = (\mathfrak{b}' : \mathfrak{I}) \cap (\mathfrak{I}' : \mathfrak{I}) = \mathfrak{b}' \cap (\mathfrak{b}' : \mathfrak{I}) \subseteq \mathfrak{b}',$$

de donde $\mathfrak{b} \subseteq \mathfrak{b}'$.

Del mismo modo, residuando $\mathfrak{a}$ por $\mathfrak{I}'$ hubiésemos encontrado $\mathfrak{b}' \subseteq \mathfrak{b}$, lo que demuestra la igualdad propuesta: $\mathfrak{b} = \mathfrak{b}'$.

Teorema 6. — *En un anillo conmutativo, las componentes aisladas de intersecciones finitas normadas de ideales primarios iguales están unívocamente determinadas.*

Corolario. — *En todas las intersecciones finitas iguales de ideales primarios normados, los ideales primarios cuyos radicales son minimales están unívocamente determinados.*

CAPÍTULO VI

AXIOMA DE ZORN

§ 1. Conjuntos inductivos; enunciado del axioma de Zorn

Dado un conjunto ordenado E interesa disponer de una condición que implique la *existencia de elementos maximales* en el mismo.

Definición. — Se llama *conjunto inductivo* a un conjunto ordenado en el cual *todo subconjunto totalmente ordenado (o cadena)* admite un *mayorante*. Entonces se introduce como axioma el siguiente:

Axioma de Zorn. — 1) *Todo conjunto inductivo admite al menos un elemento maximal.*

Si E es inductivo, el conjunto de los elementos de E superiores o iguales a un elemento a dado, es también inductivo. El axioma de Zorn, por lo tanto, implica:

1') *Todo conjunto inductivo admite al menos un elemento maximal superior o igual a un elemento dado a .*

Ejemplos de conjuntos inductivos. — a) Toda familia de Moore $\mathcal{F}$ es un conjunto inductivo, puesto que es un retículo completo, lo que exige que todo subconjunto de $\mathcal{F}$ admita un mayorante mínimo; pero la aplicación a este caso del axioma de Zorn es banal, puesto que toda familia de Moore de partes de E admite a E como elemento máximo.

b) Para las aplicaciones, el caso que corresponde a la siguiente definición es mucho más importante.

¹ Las proposiciones de Zorn, Zermelo, Hausdorff, ... que ocupan este capítulo (axiomas o teoremas, según el orden de exposición que elija cada autor) tienen un carácter peculiar debido, en resumen, a que no hay modo de construir efectivamente los entes que introducen. Aunque algún autor los califica de "métodos heterodoxos" su empleo es usual desde Steinitz (1910), E. Noether, y algebraistas sucesivos. Ahora bien, nos parece oportuno recomendar al estudiante, que en primera lectura margine las demostraciones y se limite a captar el sentido, aparentemente intuitivo, de los principios introducidos y de su mutua equivalencia, que es lo suficiente para la comprensión de capítulos posteriores. (N. del T.)

Definiciones. — Llamaremos familia $\bigcup$ -inductiva a una familia $\mathcal{U}$ de partes de E tal que la unión X^* de las partes X que pertenecen a una cadena $\mathcal{C}$ sacada de $\mathcal{U}$ sea un mayorante de los elementos de la cadena. En este caso X^* es, por construcción, mayorante mínimo de $\mathcal{C}$.

Se dice que un conjunto ordenado $\mathcal{U}$ es fuertemente inductivo si toda cadena contenida en $\mathcal{U}$ admite un mayorante mínimo.

Toda familia $\bigcup$ -inductiva es un conjunto fuertemente inductivo; todo conjunto fuertemente inductivo es inductivo.

Daremos algunos ejemplos de familias $\bigcup$ -inductivas.

1.º La familia $\mathcal{S}$ de las partes S de E estables para una aplicación α de E en E es decir $\alpha(S) \subseteq S$ es una familia $\bigcup$ -inductiva.

Sea, en efecto $\mathcal{S}'$ una subfamilia totalmente ordenada de $\mathcal{S}$. Pongamos

$$S^* = \bigcup_{S \in \mathcal{S}'} S.$$

S^* es mayorante mínimo de $\mathcal{S}'$ en $\mathcal{P}(E)$; S^* será también mayorante mínimo de $\mathcal{S}'$ en $\mathcal{S}$ si mostramos que S^* es estable para la aplicación α . Sea, pues, $s \in S^*$; existe una parte $S' \in \mathcal{S}'$ tal que $s \in S'$, de donde $\alpha(s) \in S'$ y, por lo tanto $\alpha(s) \in S^*$.

2.º Del mismo modo, las partes S estables para una familia de aplicaciones α de E en E forman una familia $\bigcup$ -inductiva. En particular si E tiene una ley de composición interna $\top$, las partes estables para toda traslación a la izquierda θ_a :

$$x \rightarrow a \top x = \theta_a(x),$$

o sea, las partes lícitas a la izquierda, forman un conjunto $\bigcup$ -inductivo.

Igualmente, la familia de las partes lícitas a la derecha, y la de las partes lícitas, son conjuntos $\bigcup$ -inductivos.

También se comprueba directamente que la familia de las partes estables para las traslaciones asociadas a los elementos de la parte, es decir, la familia de las partes de E estables para la ley de composición $\top$, es una familia $\bigcup$ -inductiva. Por lo demás, este resultado es caso particular del siguiente que vamos a demostrar.

3.º Toda familia $\mathcal{U}$ de partes de E caracterizada por una propiedad P que se refiere a un número finito p de elementos de esta parte, es una familia $\bigcup$ -inductiva.

Mostremos primero que el mayorante mínimo en $\mathcal{P}(E)$ de una cadena cualquiera $\mathcal{C}$ contenida en la familia

$$S^* = \bigcup_{S \in \mathcal{C}} S$$

pertenece a $\mathcal{U}$. Sean p elementos arbitrarios de S^* ; cada uno pertenece a por lo menos una parte $S \in \mathcal{C}$. Así se determinan p partes S , distintas o no, que forman una cadena $\mathcal{C}' \subseteq \mathcal{C}$ y una de ellas, M , contiene a las otras, luego a los p elementos considerados. Puesto que M pertenece a la familia $\mathcal{U}$, estos p elementos tienen la propiedad P . Así, p elementos arbitrarios de S^* tienen la propiedad P , luego $S^* \in \mathcal{U}$.

En el caso particular de las partes estables para una ley de composición interna T , la propiedad P se enuncia

$$a \in S \quad \text{y} \quad b \in S \quad \text{implican} \quad a T b \in S \quad (p = 2);$$

la reunión S^* de las partes estables que forman una cadena $\mathcal{C}$ es una parte estable, y la familia de partes estables es $\bigcup$ -inductiva.

Análogamente, en un grupo G la familia de los subgrupos es $\bigcup$ -inductiva; en un anillo la familia de los ideales (a la izquierda, a la derecha, biláteros) es $\bigcup$ -inductiva.

Otro ejemplo es el de las partes semiprimas S de un semigrupo D ; aquí P se enuncia:

$$\text{si existe un entero positivo } n \text{ tal que } a^n \in S, \text{ es } a \in S \text{ (aquí } p = 1).$$

En los ejemplos precedentes la familia $\mathcal{U}$ es, además, una familia de Moore. No sucede así en el ejemplo siguiente. En un conjunto ordenado $\mathcal{G}$, una cadena es una parte de $\mathcal{G}$ caracterizada por una propiedad P que se refiere a un número finito ($p = 2$) de elementos: dos elementos cualesquiera de la cadena son comparables.

El conjunto $\mathcal{U}$ de las cadenas $\mathcal{C}$ ordenadas por la inclusión de conjuntos en $\mathcal{P}(\mathcal{G})$ es, por consiguiente, $\bigcup$ -inductivo.

§ 2. Aplicaciones del axioma de Zorn

1. En todo conjunto ordenado E , existe al menos una cadena maximal, puesto que la familia de cadenas de E es $\bigcup$ -inductiva. Recíprocamente, si se supone que existe en todo conjunto ordenado E una cadena maximal $\mathcal{C}$ (axioma de Hausdorff), se deduce inmediatamente el axioma de Zorn, puesto que, si el conjunto E es inductivo, un mayorante de $\mathcal{C}$ no puede sino ser elemento máximo de $\mathcal{C}$ y elemento maximal de E .

2. Si $\mathcal{F}$ es una familia de Moore $\bigcup$ -inductiva de partes de un conjunto E , vamos a considerar, para evitar la aplicación banal del axioma de Zorn, las subfamilias $\mathcal{F}'$ de $\mathcal{F}$ que no contienen a E , pero todavía inductivas. Por lo demás, lo que sigue permanece válido si se toma como $\mathcal{F}$ una familia $\bigcup$ -inductiva que no sea, preceptivamente, una familia de Moore.

Tomemos un elemento F de $\mathcal{F}$ y una parte S de E distinta de E y no contenida en F . Sea $\mathcal{F}'$ el conjunto de las partes F' de E que pertenecen a la familia $\mathcal{F}$, contienen a F y tienen la misma intersección con S que F :

$$\mathcal{F}' = \{ F' ; F' \in \mathcal{F} ; F' \supseteq F, F' \cap S = F \cap S \}, \quad (S \neq E, S \not\subseteq F \in \mathcal{F})$$

Lema. — Se tiene $\mathcal{F}' \neq \emptyset$; $E \notin \mathcal{F}'$. La familia $\mathcal{F}'$ es un conjunto $\bigcup$ -inductivo.

$\mathcal{F}'$ no es vacío, puesto que $F \in \mathcal{F}'$. Como $E \cap S = S \neq F \cap S$, E no pertenece a $\mathcal{F}'$. Una cadena $\mathcal{C}$ extraída de $\mathcal{F}'$ admite, en $\mathcal{F}$, un mayorante mínimo H , unión de los elementos de la cadena

$$H = \bigcup_{X \in \mathcal{C}} X.$$

Ahora bien, tenemos $F \subseteq X, \forall X \in \mathcal{C} (\subseteq \mathcal{F}')$, luego $F \subseteq H$, y, de otra parte

$$H \cap S = \left(\bigcup_{X \in \mathcal{C}} X \right) \cap S = \bigcup_{X \in \mathcal{C}} (X \cap S) = F \cap S.$$

Luego $H \in \mathcal{F}'$ y $\mathcal{F}'$ es un conjunto $\bigcup$ -inductivo.

Esta propiedad implica, por el axioma de Zorn, que $\mathcal{F}'$ tiene al menos un elemento maximal. Hemos establecido así el siguiente

Teorema 1. — Sean $\mathcal{F}$ una familia $\bigcup$ -inductiva de partes de un conjunto E , F un elemento particular de esta familia y S un subconjunto propio de E no contenido en F . Entre los elementos de la familia $\mathcal{F}$ que contienen a F y cortan a S según $S \cap F$, existe al menos una parte maximal M .

Si, en particular, S es disjunto de F , es decir, si $S \cap F = \emptyset$, hay en la familia $\mathcal{F}$, entre los elementos que contienen a F y disjuntos con S , un elemento maximal M .

Ejemplo 1. — Supongamos que E sea un anillo R con elemento unidad e . Sea $\mathcal{F}$ la familia no vacía de los ideales biláteros distintos de R . Tomemos $S = \{e\}$. El teorema 1 da:

Teorema 2. — Para todo ideal bilátero $\mathfrak{a}$ de R , existe un ideal maximal $\mathfrak{m} \neq R$ (cf. cap. IV, § 8) que contiene a $\mathfrak{a}$.

Para los ideales a la derecha, o a la izquierda, vale el enunciado análogo.

Si consideramos en particular un anillo de Boole (cap. V, § 7), veremos que todo filtro está contenido en un filtro maximal (o ultrafiltro). Esta propiedad se obtiene también aplicando el teorema 1 a la familia $\mathcal{F}$ de los filtros propios, es decir, de las partes de $\mathcal{P}(E)$ estables para la intersección $\cap$, lícitas para la unión y sin incluir a $\emptyset$.

Ejemplo 2. — Sea $\mathcal{F}$ una familia $\bigcup$ -inductiva de partes de un conjunto E , F un elemento de $\mathcal{F}$ distinto de E , x un elemento de E no perteneciente a F . Tomemos $S = \{x\}$, luego $S \cap F = \emptyset$.

Existe una parte maximal F_x perteneciente a $\mathcal{F}$, que contiene a F y que no contiene a x .

Teorema 3. — F_x es, en la familia $\mathcal{F}$, un elemento $\bigcap$ -irreducible; es decir, que no es la intersección de dos elementos F', F'' de $\mathcal{F}$ que le contengan estrictamente.

Puesto que x no pertenece a F_x la igualdad $F_x = F' \cap F''$ implica, por ejemplo, $x \notin F'$. Pero conteniendo F' a F_x y no conteniendo a x , no puede contener estrictamente a F_x , que es maximal.

Tenemos $F' = F_x$, y F_x es efectivamente $\bigcap$ -irreducible.

Así, para todo $x \notin F$, ($F \in \mathcal{F}$), existe un elemento $\bigcap$ -irreducible F_x de $\mathcal{F}$ que contiene a F y no contiene a x ; es claro que

$$F = \bigcap_{x \in \mathbb{C}_E F} F_x$$

y tenemos, en consecuencia, la proposición siguiente:

Teorema 4. — En una familia $\bigcup$ -inductiva $\mathcal{F}$ de partes de E , todo elemento F de $\mathcal{F}$ es intersección de elementos $\bigcap$ -irreducibles que le contienen, y, en consecuencia, intersección de todos los elementos $\bigcap$ -irreducibles que le contienen.

En particular, en todo anillo A (conmutativo o no, con o sin elemento unidad), todo ideal bilátero, es la intersección de los ideales $\bigcap$ -irreducibles que le contienen (vale el enunciado análogo para los ideales a la derecha, o a la izquierda).

Estudiemos la familia $\mathcal{P}$ de los ideales primos $\mathfrak{p}$ que contienen a un ideal dado $\mathfrak{a}$. Si r es un elemento del radical $\mathcal{R}(\mathfrak{a})$, existe un entero n tal que $r^n \in \mathfrak{a} \subseteq \mathfrak{p}$, de donde $r \in \mathfrak{p}$, y $\mathfrak{p}$ contienen al radical $\mathcal{R}(\mathfrak{a})$. Como, recíprocamente, todo ideal primo que contiene a $\mathcal{R}(\mathfrak{a})$ contiene a $\mathfrak{a}$, la familia $\mathcal{P}$ de los ideales primos que contienen a $\mathfrak{a}$ coincide con la de los que contienen a $\mathcal{R}(\mathfrak{a})$.

Teorema 5. — Todo ideal semiprimo $\mathfrak{r}$ es la intersección de los ideales primos que lo contienen. El radical $\mathcal{R}(\mathfrak{a})$ de un ideal $\mathfrak{a}$ es la intersección de los ideales primos que contienen a $\mathfrak{a}$.

Basta con establecer la primera parte del enunciado que, según la observación precedente, implica inmediatamente la segunda.

Sea $\mathcal{P}$ la familia de los ideales primos $\mathfrak{p}$ que contienen al ideal semiprimo $\mathfrak{r}$; pongamos $\mathfrak{i} = \bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}$. Tenemos entonces $\mathfrak{r} \subseteq \mathfrak{i}$, y demostraremos la igualdad viendo que $x \notin \mathfrak{r}$ implica $x \notin \mathfrak{i}$.

El conjunto $X = \{x, x^2, \dots, x^n, \dots\}$ de las potencias de x es una parte multiplicativamente estable, y disjunta de $\mathfrak{r}$, puesto que $\mathfrak{r}$ es semiprimo. Basta entonces probar que existe un ideal $\mathfrak{m}$ primo, que contiene a $\mathfrak{r}$ y es disjunto con X : tendremos entonces $x \notin \mathfrak{m}$ y, puesto que $\mathfrak{m} \in \mathcal{P}$, $x \notin \mathfrak{i}$.

Ahora bien, según el teorema 1 (aplicado a la familia $\bigcup$ -inductiva $\mathcal{F}$ de los ideales de A , al ideal $\mathfrak{r}(= F)$ y a la parte $X(= S)$ disjunta con $\mathfrak{r}$), existe un ideal $\mathfrak{m}$ que es maximal entre los que contienen a $\mathfrak{r}$ y son disjuntos con X ; veamos que este ideal $\mathfrak{m}$ es primo.

Supongamos que existiesen dos elementos a, b del anillo A cumpliendo las condiciones

$$ab \in \mathfrak{m}, \quad a \notin \mathfrak{m}, \quad b \notin \mathfrak{m}.$$

Puesto que $\mathfrak{m}$ es maximal en la familia $\mathcal{F}$, tendremos $\mathfrak{m} + (a) \notin \mathcal{F}$ y como $\mathfrak{m} + (a)$ contiene a $\mathfrak{r}$, ello exige

$$[\mathfrak{m} + (a)] \cap X \neq \emptyset$$

Sea pues x_1 un elemento de X perteneciente a $\mathfrak{m} + (a)$ y, lo mismo, x_2 un elemento de X perteneciente a $\mathfrak{m} + (b)$. Tenemos $x_1 x_2 \in X$ y

$$x_1 x_2 \in [\mathfrak{m} + (a)] [\mathfrak{m} + (b)] \subseteq \mathfrak{m} + (ab) \subseteq \mathfrak{m},$$

lo que es contradictorio; $\mathfrak{m}$ es en efecto un ideal primo.

Volvamos a la familia $\mathcal{F}$ de los ideales primos que contienen a $\mathfrak{a}$ o a $\mathcal{R}(\mathfrak{a})$. Es claro que todo ideal de esta familia que contenga a otro es superfluo en la formación de la intersección $\mathfrak{i} = \bigcap_{\mathfrak{p} \in \mathcal{F}} \mathfrak{p}$. Vamos a establecer el teorema siguiente:

Teorema 6. — *Todo ideal $\mathfrak{p}$ primo que contiene a $\mathfrak{a}$ contiene un elemento minimal, $\bar{\mathfrak{p}}$ de la familia $\mathcal{F}$ de los ideales primos que contienen a $\mathfrak{a}$. Si $\bar{\mathcal{F}}$ es la familia de los ideales $\bar{\mathfrak{p}}$ primos que contienen a $\mathfrak{a}$ minimales, se tiene*

$$\mathcal{R}(\mathfrak{a}) = \bigcap_{\bar{\mathfrak{p}} \in \bar{\mathcal{F}}} \bar{\mathfrak{p}}.$$

La segunda parte del enunciado es una consecuencia inmediata de la primera. Para esta vamos a dar dos demostraciones.

Primera demostración. — El conjunto complementario de $\mathfrak{p}$, $A - \mathfrak{p} = X$, es estable multiplicativamente, puesto que $\mathfrak{p}$ es primo. La familia $\mathcal{X}$ de las partes de A multiplicativamente estables, conteniendo a X y disjuntas de $\mathcal{R}(\mathfrak{a})$ es $\bigcup$ -inductiva; en ella hay un elemento maximal $\bar{X}$.

Según el lema, la familia $\bar{\mathcal{F}}$ de los ideales que contienen a $F = \mathcal{R}(\mathfrak{a})$ y son disjuntos de $\bar{X}$, admite un elemento maximal que es un ideal primo $\bar{\mathfrak{p}}$; $\bar{\mathfrak{p}}$ pertenece a la familia $\mathcal{F}$. $A - \bar{\mathfrak{p}}$ es disjunto de $\mathcal{R}(\mathfrak{a})$ y multiplicativamente estable; además $A - \bar{\mathfrak{p}}$ contiene a $\bar{X}$, luego a X , luego pertenece a la familia $\mathcal{X}$. Por ser $\bar{X}$ maximal en esta familia tenemos $A - \bar{\mathfrak{p}} = \bar{X}$.

$\bar{X} \supseteq X$ implica entonces $\bar{\mathfrak{p}} \supseteq \mathfrak{p}$; además, siendo $\bar{X}$ maximal en la familia $\mathcal{X}$, $\bar{\mathfrak{p}}$ es minimal en la familia $\mathcal{F}$.

Segunda demostración. — Consideremos la familia $\mathcal{F}'$ de los ideales primos del anillo A que contienen al radical $\mathcal{R}(\mathfrak{a})$ y contenidos en $\mathfrak{p}$. Ordenémosla poniendo $\mathfrak{p}'_1 \leq \mathfrak{p}'_2$ si $\mathfrak{p}'_2 \subseteq \mathfrak{p}'_1$ (orden opuesto a la inclusión).

Si consideramos una cadena $\mathcal{C}$ extraída de $\mathcal{F}'$ y el ideal $\mathfrak{r} = \bigcap_{\mathfrak{p}' \in \mathcal{C}} \mathfrak{p}'$, este ideal $\mathfrak{r}$ es *primo*. Supongamos, en efecto, $ab \in \mathfrak{r}$, y $a \notin \mathfrak{r}$. Existe un ideal $\mathfrak{p}'_1 \in \mathcal{C}$ tal que $a \notin \mathfrak{p}'_1$ y entonces tenemos $a \notin \mathfrak{p}'$ para todo ideal $\mathfrak{p}'$ de $\mathcal{C}$ que cumpla $\mathfrak{p}' \subseteq \mathfrak{p}'_1$; y en consecuencia $b \in \mathfrak{p}'$ para todo $\mathfrak{p}' \subseteq \mathfrak{p}'_1$, pero entonces b pertenece a $\mathfrak{p}'_1$ y también a todo ideal de $\mathcal{C}$ que contenga a $\mathfrak{p}'_1$; finalmente, b pertenece a todos los ideales de la cadena $\mathcal{C}$, luego $b \in \mathfrak{r}$.

El ideal $\mathfrak{r}$ es, en el orden $\leq$, mayorante mínimo de la cadena $\mathcal{C}$ y en consecuencia el conjunto $\mathcal{F}'$ es inductivo. Según el axioma de Zorn existe en $\mathcal{F}'$ un elemento $\mathfrak{p}$ maximal para el orden $\leq$, y este ideal responde a la cuestión.

§ 3. Axiomas equivalentes al de Zorn

Definición. — Se dice que un conjunto E está *bien ordenado* (o que tiene un *buen orden*) si la ordenación es tal que cualquier parte no vacía de E tiene un elemento mínimo. En consecuencia estará *totalmente ordenado*, porque si la parte $\{a, b\}$ tiene un elemento mínimo, dos elementos cualesquiera a, b , serán comparables. Todo subconjunto A de un conjunto bien ordenado E es evidentemente bien ordenado (para la restricción a A del orden de E). Todo orden total sobre un conjunto finito es un buen orden para este conjunto (es decir, le hace bien ordenado). Sin el axioma de Zorn, o un axioma equivalente, no se sabe si todo conjunto puede ser bien ordenado.

Si E es un conjunto cualquiera, consideremos los pares (A, O_A) formados por un subconjunto A que se sepa ordenar bien, y un buen orden O_A de A . El conjunto $\mathcal{M}$ de estos pares no es vacío, puesto que comprende todas las disposiciones p a p en los subconjuntos finitos F de n elementos de E , cualesquiera sean n y p ($p \leq n$).

Definamos en $\mathcal{M}$ la relación de orden Ω , indicada por $\leq$, siguiente:

$$(\Omega) \quad (A, O_A) \leq (B, O_B) \quad \text{si} \quad \begin{cases} 1) A \subseteq B, \\ 2) O_A \text{ es la restricción a } A \text{ de } O_B, \\ 3) a \in A, \quad b \in B, \quad b < a \quad \text{para } O_B, \\ \quad \text{implican } b \in A. \end{cases}$$

Como se ve inmediatamente, la relación definida en $\mathcal{M}$ por estas tres condiciones es *reflexiva*, *transitiva* y *antisimétrica*: es pues, realmente, una relación de orden.

Partiremos entonces de la observación siguiente:

Si $\mathcal{M}$ tiene un elemento maximal, el conjunto E puede ser bien ordenado y reciprocamente. Son, pues, equivalentes, las dos propiedades del enunciado.

Supongamos primero que un par (A, O_A) sea elemento maximal de $\mathcal{M}$ y mostremos que $A = E$. En caso contrario, sea b un elemento de E no perteneciente a A ; sobre $B = A \cup \{b\}$, el orden O_B que coincide con O_A sobre A y es tal que

$$a \leq b \quad \forall a \in A$$

es un buen orden de B y da un par (B, O_B) mayor que (A, O_A) , contra la hipótesis.

Ahora, si O_E es un buen orden de E , es claro que el par (E, O_E) es elemento maximal de $\mathcal{M}$ puesto que dos pares en que interviene el mismo conjunto son iguales si su buen orden es el mismo, y no son comparables en el caso contrario.

Lema. — *El conjunto $\mathcal{M}$ ordenado por el orden Ω , es inductivo.*

Sea $\mathcal{C}$ una cadena sacada de $\mathcal{M}$. Consideremos la familia $\mathcal{F}$ de las partes A figurando en los pares (A, O_A) de $\mathcal{C}$; $\mathcal{F}$ es ella misma una cadena (para la relación de inclusión). Sea $R = \bigcup_{A \in \mathcal{F}} A$ la reunión de las partes A de E que

pertenecen a $\mathcal{F}$. Ordenemos R de la manera siguiente.

Consideremos un número finito n de elementos de $R, r_1, r_2, \dots, r_n$ y, para cada índice i , un conjunto $A_i \in \mathcal{F}$ tal que $r_i \in A_i$. Como $\mathcal{F}$ es una cadena, uno de los conjuntos A_i , que llamaremos A , contiene a todos los otros; tenemos pues $r_i \in A$ cualquiera sea $i \in \{1, 2, \dots, n\}$. Si B es otro conjunto de la familia $\mathcal{F}$ que contiene igualmente a $r_1, r_2, \dots, r_n$, la relación $r_i \leq r_j$ en el orden O_A , donde $i, j \in \{1, 2, \dots, n\}$, implica la relación $r_i \leq r_j$ en el orden O_B puesto que $\mathcal{C}$ es una cadena.

Tomemos n igual a 2 y definamos el orden O_R poniendo $r_1 \leq r_2$ en O_R si se tiene, conforme a lo que precede $r_1 \leq r_2$ en O_A , siendo A cualquier conjunto de la familia $\mathcal{F}$ que contenga a r_1 y r_2 . Esta relación O_R es desde luego reflexiva y antisimétrica; también es transitiva, lo que se ve inmediatamente tomando $n = 3$ en el razonamiento anterior. Además este orden O_R es según su definición un *orden total*.

Mostremos que el orden O_R así definido es un buen orden. Sea S una parte no vacía de R : debemos mostrar que S tiene un elemento mínimo. Sea s un elemento de S ($\neq \emptyset$ por hipótesis). O bien s es elemento mínimo de S en el orden O_R (y entonces la propiedad queda establecida), o bien el conjunto T de los elementos t de S que preceden a s en este orden no es vacío. Sea (A, O_A) un

par de la cadena $\mathcal{C}$ tal que $s \in A$; si t designa un elemento cualquiera de T , sea (B, O_B) un par de $\mathcal{C}$ tal que $t \in B$. Puesto que $\mathcal{F}$ es una cadena, tenemos o bien $B \subseteq A$, y entonces $t \in A$, o bien $A \subset B$, y entonces $s \in A$, $t \in B$, $t < s$ en el orden O_R , luego en el orden O_B implican, según la definición de Ω , $t \in A$. Así, de todos modos, $t \in A$; en consecuencia, tenemos $T \subseteq A$.

Como parte no vacía del conjunto bien ordenado A , T admite un elemento mínimo m en el orden O_A ; pero las restricciones a T ($\subseteq A \subseteq R$) de los órdenes O_A y O_R coinciden, luego T admite a m como elemento mínimo en el orden O_R . Puesto que O_R es un orden total, m es también elemento mínimo de S , luego O_R es un buen orden.

Así el par (R, O_R) pertenece al conjunto $\mathcal{M}$. Además mayora a la cadena $\mathcal{C}$:

$$(A, O_A) \leq (R, O_R) \quad \text{en el orden } \Omega, \quad \forall (A, O_A) \in \mathcal{C};$$

tenemos en efecto, por construcción, $A \subseteq R$ y O_A es la restricción de O_R a A . Sea por otra parte $a \in A$, $x \in R$, $x < a$ en el orden O_R . Existe en la cadena $\mathcal{F}$ un conjunto X que contiene x y A , y si (X, O_X) es el par correspondiente de la cadena $\mathcal{C}$, se tiene necesariamente

$$(A, O_A) \leq (X, O_X) \quad \text{en el orden } \Omega$$

pero entonces, la desigualdad $x < a$ en O_X (restricción de O_R a X) implica $x \in A$.

Igualmente, puesto que R es mayorante mínimo de la cadena $\mathcal{F}$, el par (R, O_R) es mayorante mínimo de la cadena $\mathcal{C}$. El conjunto $\mathcal{M}$, con el orden Ω , es fuertemente inductivo, luego es inductivo.

Con esto, según el axioma de Zorn, $\mathcal{M}$ tiene un elemento maximal y según la observación preliminar, existe, en el conjunto E , un buen orden.

La proposición:

(II) *todo conjunto E puede ser bien ordenado*, se conoce con el nombre de axioma de Zermelo. En virtud del lema precedente, podemos enunciar

Teorema 1. — *El axioma de Zorn (I) implica como consecuencia el axioma de Zermelo (II).*

Otro axioma fundamental es el *axioma de elección*; he aquí su enunciado:

(III) *Para todo conjunto E , se puede definir una función de elección f , es decir, una aplicación de $\mathfrak{P}(E)$ en E que asocia a toda parte no vacía A de E un elemento $a = f(A)$ de E perteneciente a A ("elemento distinguido" de A).*

Es evidente que, si un conjunto E tiene una buena ordenación se puede definir una función de elección: basta asociar a toda parte A no vacía de E su mínimo elemento. Luego:

Teorema 2. — *El axioma de Zermelo (II) implica el axioma de elección (III). Nos falta establecer otra equivalencia:*

Teorema 3. — *El axioma de elección (III) implica el axioma de Zorn.*

Sea H una parte de un conjunto ordenado E ; designemos por $\overset{>}{H}$ el conjunto de elementos del complementario $\complement_E H$ que son mayorantes de H :

$$\overset{>}{H} = \{x; x \in E, x \notin H; \forall h \in H, h < x\}.$$

Supongamos definida una *función de elección* en el conjunto ordenado E ; sea f esta función.

Definición. — Diremos que una cadena K contenida en E es una *k-cadena* si, para toda parte hereditaria H de K , distinta de K , el elemento distinguido $f(\overset{>}{H})$ es elemento mínimo de $\overset{>}{H} \cap K$.

Al ser H parte hereditaria de K , el complemento de H en la cadena K está contenido en $\overset{>}{H}$; por tanto, la condición $H \neq K$ es equivalente a $\overset{>}{H} \cap K \neq \emptyset$.

Tomemos $H = \emptyset$, entonces $\overset{>}{H} = E$, $\overset{>}{H} \cap K = K$ y la definición de *k-cadena* da: $e = f(\overset{>}{H}) = f(E)$ es elemento mínimo de K . Así, todas las *k-cadenas* admiten $e = f(e)$ como elemento mínimo. Por lo demás, $\{e\}$ es una *k-cadena*, pues es una cadena C cuya única parte hereditaria diferente de C es $\emptyset$; acabamos de ver que $f(\overset{>}{\emptyset}) = f(E) = e$, y e es en efecto elemento mínimo de $\overset{>}{\emptyset} \cap \{e\} = E \cap \{e\} = \{e\}$.

Teorema 4. — *En el conjunto $\mathcal{C}$ de todas las cadenas (ordenado por inclusión), el conjunto $\mathcal{K}$ de las k-cadenas es una cadena; cada k-cadena es parte hereditaria de toda k-cadena que la contenga.*

Consideremos dos *k-cadenas*, K_1, K_2 , y sea

$$I = \{x; x \in K_1 \cap K_2, K_1 \cap \overset{\leq}{x} = K_2 \cap \overset{\leq}{x}\}.$$

El conjunto I no es vacío, puesto que $e \in I$.

Mostremos primero que I es parte hereditaria de K_1 (luego, también de K_2). Sean $i \in I, k_1 \in K_1, k_1 < i$. Tenemos:

$$K_1 \cap \overset{\leq}{i} = K_2 \cap \overset{\leq}{i},$$

pero $k_1 \in K_1 \cap \overset{\leq}{i}$, luego $k_1 \in K_2 \cap \overset{\leq}{i}$, de donde $k_1 \in K_1 \cap K_2$.

Además,
$$K_1 \cap \overset{\leq}{i} \cap \overset{\leq}{k_1} = K_2 \cap \overset{\leq}{i} \cap \overset{\leq}{k_1}$$

lo que se escribe, puesto que $k_1 < i$,

$$K_1 \cap \overset{\leq}{k_1} = K_2 \cap \overset{\leq}{k_1}.$$

En fin, $k_1 \in I$; I es efectivamente parte hereditaria de K_1 y también de K_2 .

Además, *no puede ser al tiempo* $I \neq K_1$ e $I \neq K_2$. Supongamos, en efecto, ambas desigualdades. Puesto que K_1 y K_2 son k -cadenas, $m = f(\overset{>}{I})$ es entonces elemento mínimo de $\overset{>}{I} \cap K_1$ y de $\overset{>}{I} \cap K_2$. Puesto que I es parte hereditaria de K_1 y que existe un mínimo mayorante escrito, m , de I en K_1 , tenemos:

$$I = K_1 \cap \overset{<}{m} \quad \text{y lo mismo} \quad I = K_2 \cap \overset{<}{m}.$$

Resulta: $(K_1 \cup \overset{<}{m}) \cup \{m\} = (K_2 \cap \overset{<}{m}) \cup \{m\}$, es decir:

$$K_1 \cap \overset{\leq}{m} = K_2 \cap \overset{\leq}{m}$$

luego $m \in I$, en contradicción con $m \in \overset{>}{I}$. Tenemos, pues, $I = K_1$ o $I = K_2$ y una de las dos cadenas K_1, K_2 es parte hereditaria de la otra. Con esto queda demostrado el Teorema 4.

Teorema 5. — *La unión de las k -cadenas*

$$K^* = \bigcup_{K \in \mathcal{K}} K$$

es una k -cadena.

K^* es evidentemente una cadena. Demostremos que es una k -cadena: Sea H una parte hereditaria de K^* distinta de K^* , luego $\overset{>}{H} \cap K^* \neq \emptyset$. Vamos a establecer que $f(\overset{>}{H}) = s$ es elemento mínimo de $\overset{>}{H} \cap K^*$. Sea $k \in \overset{>}{H} \cap K^*$; mostremos que se tiene: $s \leq k$. Puesto que $k \in K^*$, existe una k -cadena $K_i \in \mathcal{K}$ tal que $k \in K_i$ y puesto que $k \in \overset{>}{H}$, k es un elemento de K_i que mayor a H y no le pertenece. Demostremos que H está contenido en K_i (y entonces estrictamente, puesto que $k \in K_i$, $k \notin H$). Si tuviésemos $h \in H$, $h \notin K_i$, como existe una k -cadena K_λ conteniendo a h , K_i sería, según el Teorema 4, parte hereditaria de K_λ . Pero entonces h sería una mayorante de K_i no perteneciéndole, por lo que tendríamos $h > k$; y siendo H por hipótesis parte hereditaria de K^* , resultaría $k \in H$, lo que es contradictorio. Esto dicho, la inclusión $H \subset K_i$ ($\subseteq K^*$) implica, puesto que H es parte hereditaria de K^* , que H es parte hereditaria de K_i ; entonces, puesto que $K_i f \neq \overset{>}{H}$, $(H) = s$ es elemento mínimo de $\overset{<}{H} \cap K_i$, de donde $s \leq k$, como queríamos demostrar.

Corolario. — *Se tiene:*

$$\vec{K}^* = \emptyset$$

En efecto, si fuese $\vec{K}^* \neq \emptyset$, entonces $K^* \cup \{f(\vec{K}^*)\}$ sería una cadena y precisamente, como ahora vamos a ver, una k -cadena, lo que no es posible. El hecho de que $K^* \cup f(\vec{K}^*)$ sería una k -cadena resulta de la proposición general siguiente:

Lema. — *Si K es una k -cadena y si tenemos: $\vec{K} \neq \emptyset$, entonces $K \cup f(\vec{K})$ es también una k -cadena.*

Sea en efecto H una parte hereditaria propia de $K \cup f(\vec{K})$, lo que implica $f(\vec{K}) \notin H$; tenemos, pues, $H \subseteq K$. Entonces:

si $H = K$, tenemos $f(\vec{H}) = f(\vec{K})$, que es efectivamente elemento mínimo de $\vec{H} \cap [K \cup f(\vec{K})] = \{f(\vec{K})\}$;

si $H \subset K$, siendo K una k -cadena, $f(\vec{H})$ es elemento mínimo de $\vec{H} \cap K$, luego, *a fortiori*, de $\vec{H} \cap [K \cup f(\vec{K})] = (\vec{H} \cap K) \cup f(\vec{K})$, que sólo difiere por la adjunción del mayorante $f(\vec{K})$.

Con esto queda establecido el Lema y, por tanto, también el Corolario.

La teoría de las k -cadenas nos proporciona, pues, una cadena K^* que no admite ningún mayorante que no le pertenezca.

Si el conjunto E es inductivo, K^* es mayorada; tiene, pues, según lo precedente, un elemento máximo, el cual es además *elemento maximal* de E .

Por tanto, el axioma de Zorn resulta de la existencia de una función de elección: el Teorema 3 queda demostrado.

Nota. — De la equivalencia de los axiomas (I), (II) y (III) resulta en particular que, mediante el axioma de elección, todo conjunto puede ser bien ordenado. Esta proposición es el Teorema de Zermelo.

CAPÍTULO VII

ANILLOS NOETHERIANOS

§ 1. Retículos con condiciones de cadena

Definición. — Se dice que un conjunto ordenado E satisface a la *condición maximal* si todo subconjunto no vacío de E tiene al menos un elemento maximal.

Teorema 1. — *Un conjunto ordenado E satisface a la condición maximal si, y sólo si, todo subconjunto totalmente ordenado de E admite un elemento máximo.*

1) Si E satisface a la condición maximal, todo subconjunto totalmente ordenado de E admite un elemento maximal. Pero un elemento maximal de una cadena es elemento máximo y todo subconjunto totalmente ordenado de E admite un elemento máximo.

2) Recíprocamente, sea E' un subconjunto no vacío de E . Todo subconjunto totalmente ordenado de E' es subconjunto totalmente ordenado de E y en consecuencia admite, por hipótesis, un elemento máximo (que pertenece a E'). E' es pues inductivo; luego, mediante el axioma de Zorn, E' tiene un elemento maximal y E satisface a la condición maximal.

Teorema 2. — *Un sup-semirretículo $\mathfrak{C}$ que satisface a la condición maximal es completo y toda unión es una unión finita.*

En efecto, sea S un subconjunto no vacío cualquiera de $\mathfrak{C}$. Consideremos el conjunto S^* de todas las uniones finitas de elementos de S : $S \subseteq S^* \subseteq \mathfrak{C}$. Por la condición maximal, S^* tiene al menos un elemento maximal u^* . Existe pues una unión finita de elementos de S tal que

$$s_1 \vee s_2 \vee \dots \vee s_n = u^* \quad \text{y si } s \in S, \quad s \vee u^* = u^*$$

puesto que u^* es maximal; luego $s \leq u^*$, $\forall s \in S$. Luego u^* es mayorante de S .

Pero por construcción u^* es *mayorante mínimo* de $S' = \{s_1, s_2, \dots, s_n\}$, luego *a fortiori* de S .

Consideremos en particular un anillo conmutativo A para el cual el retículo de los ideales $\mathfrak{I}$ verifica la condición maximal.

Definición. — Se llama *anillo noetheriano* (de Noether) un anillo A en que *todo ideal $\mathfrak{m}$ admite una base finita* (es decir un sistema finito de generadores):

$$\mathfrak{m} = (m_1, \dots, m_r)$$

Si suponemos A conmutativo, $\mathfrak{m}$ es el conjunto de sumas

$$\sum_{i=1}^r \nu_i m_i + a_i m_i \quad (\nu_i \in \mathbb{Z}, a_i \in A)$$

y si A tiene elemento unidad, el conjunto de sumas

$$\sum_{i=1}^r a_i m_i.$$

Teorema 3. — *Si el retículo de los ideales de un anillo A (conmutativo) verifica la condición maximal, el anillo A es noetheriano.*

En efecto, todo ideal $\mathfrak{m}$ de A es, en el retículo completo $\mathfrak{G}$ de los ideales de A , la unión de los ideales principales engendrados por sus elementos, luego, según el teorema 2, es unión finita de tales ideales principales:

$$\mathfrak{m} = (a_1) \vee \dots \vee (a_n) = (a_1) + \dots + (a_n) = (a_1, \dots, a_n).$$

recíprocamente:

Teorema 4. — *El retículo de los ideales de un anillo noetheriano A verifica la condición maximal.*

Bastará mostrar que toda familia totalmente ordenada $\mathcal{C}$ de ideales de A admite un elemento máximo. Ahora bien, la reunión $\mathfrak{m}^* = \bigcup_{\mathfrak{m} \in \mathcal{C}} \mathfrak{m}$ es un ideal, mayorante mínimo de la familia $\mathcal{C}$ (cap. IV, § 1). Siendo A noetheriano por hipótesis, $\mathfrak{m}^*$ admite una base finita: $\mathfrak{m}^* = (m_1, \dots, m_r)$ y como m_i pertenece a la reunión $\bigcup_{\mathfrak{m} \in \mathcal{C}} \mathfrak{m}$, existe al menos un ideal $\mathfrak{m}_i \in \mathcal{C}$ tal que $m_i \in \mathfrak{m}_i$. Siendo $\mathcal{C}$ una

cadena, uno de los ideales $\mathfrak{m}_1, \dots, \mathfrak{m}_r$, sea $\mathfrak{m}_\alpha$, contiene a todos los otros y tenemos $\mathfrak{m}_i \subseteq \mathfrak{m}_\alpha$ ($i=1, \dots, r$), de donde $\mathfrak{m}^* \subseteq \mathfrak{m}_\alpha$. Ahora bien $\mathfrak{m}_\alpha \in \mathcal{C}$ y por consiguiente tenemos $\mathfrak{m}_\alpha \subseteq \mathfrak{m}^*$, de donde la igualdad $\mathfrak{m}_\alpha = \mathfrak{m}^*$ luego $\mathfrak{m}^*$ pertenece a $\mathcal{C}$ y es elemento máximo.

Volvamos a un conjunto ordenado cualquiera E .

Definición. — Se dice que un conjunto ordenado E verifica o cumple la *condición de cadena ascendente*, si toda sucesión de elementos de E subindicada por los enteros naturales y estrictamente creciente

$$a_1 < a_2 < \dots$$

es *finita*. Esta condición es equivalente a la siguiente: En toda sucesión infinita débilmente creciente $x_1 \leq x_2 \leq \dots \leq x_n \leq x_{n+1} \leq \dots$, vale el signo de igualdad a partir de un cierto lugar de orden.

Teorema 5. — *La condición maximal implica la condición de cadena ascendente. Recíprocamente, mediante el axioma de elección (equivalente al axioma de Zorn), la condición de cadena ascendente implica la condición maximal.*

La primera parte es evidente: una sucesión estrictamente creciente ilimitada $a_1 < a_2 < \dots < a_n < \dots$ debe admitir, por la condición maximal, un elemento máximo a_k , lo que es contradictorio puesto que $a_k < a_{k+1}$.

Supongamos ahora que E cumple la condición de cadena ascendente; sea E' un subconjunto totalmente ordenado de E , y veamos que E' tiene un elemento máximo. Existe, según el axioma de la hipótesis, una función de elección en E' , es decir una función f que asocia a toda parte no vacía X de E' un elemento $x \in X$, $x = f(X)$. Pongamos $e_1 = f(E')$. Si e_1 es elemento máximo de E' la proposición queda establecida. Si no, la sección inicial S_1 de e_1 , en E' ,

$$S_1 = \{x; x \in E', x \leq e_1\},$$

no agota a E' : pongamos $e_2 = f(E' - S_1)$; tenemos $e_1 < e_2$. El razonamiento se reitera: si se han obtenido n elementos e_i formando una sucesión estricta creciente

$$e_1 < e_2 < \dots < e_n$$

y si e_n no es elemento máximo de E' , $E' - S_n$, donde S_n es la sección inicial de e_n en E' , no es vacío y se tiene $e_n < e_{n+1} = f(E' - S_n)$. Según la condición de cadena ascendente, el proceso se detiene para un cierto valor k de n , y por consecuencia E' tiene e_k como elemento máximo.

Se define de un modo análogo la *condición minimal* (un conjunto ordenado E satisface a la condición minimal si todo subconjunto no vacío de E tiene al menos un elemento minimal) y la *condición de cadena descendente* (toda sucesión estrictamente decreciente $a_1 > a_2 > \dots$ de elementos de E es necesariamente finita) y se establece su equivalencia.

§ 2. Anillos noetherianos

En todo lo que sigue se trata de anillos conmutativos noetherianos y damos por sobreentendida la palabra conmutativo.

Comenzaremos el estudio de los anillos noetherianos por un importante *teorema de transferencia* debido a Hilbert.

Teorema 1 (teorema de la base finita). — Si R es un anillo noetheriano con elemento unidad e , el anillo $P = R[x]$ de los polinomios en x con coeficientes en R es noetheriano.

Demostraremos este teorema haciendo ver que P cumple la condición de cadena ascendente. En primer lugar daremos un lema:

Lema 1. — Sea $\mathfrak{a}$ un ideal del anillo P ; el conjunto $C_n(\mathfrak{a})$ formado por el cero de R , 0, y por los coeficientes de x^n en los polinomios de grado n que pertenecen a $\mathfrak{a}$, es un ideal del anillo R ; los ideales $C_n(\mathfrak{a})$ forman una sucesión débilmente creciente:

$$C_0(\mathfrak{a}) \subseteq C_1(\mathfrak{a}) \subseteq \dots \subseteq C_n(\mathfrak{a}) \subseteq C_{n+1}(\mathfrak{a}) \subseteq \dots$$

Sean a, b dos elementos de $C_n(\mathfrak{a})$, es decir

$$\begin{aligned} f &= ax^n + a_1x^{n-1} + \dots \in \mathfrak{a} \\ g &= bx^n + b_1x^{n-1} + \dots \in \mathfrak{a} \end{aligned}$$

resulta

$$f - g = (a - b)x^n + (a_1 - b_1)x^{n-1} + \dots \in \mathfrak{a}$$

y el elemento $a - b$, sea nulo o sea diferente de cero, pertenece al conjunto $C_n(\mathfrak{a})$. Por otra parte, para todo elemento r de R , tenemos

$$rf = (ra)x^n + ra_1x^{n-1} + \dots \in \mathfrak{a}$$

y el elemento ra , sea nulo o distinto de cero, pertenece a $C_n(\mathfrak{a})$; $C_n(\mathfrak{a})$ es, pues, un ideal en el anillo R .

Como R tiene elemento unidad e , $x = ex$ es un polinomio de P y tenemos

$$xf = ax^{n+1} + a_1x^n + \dots \in \mathfrak{a}$$

luego todo elemento a de $C_n(\mathfrak{a})$ pertenece a $C_{n+1}(\mathfrak{a})$, los ideales $C_n(\mathfrak{a})$ forman una cadena débilmente creciente.

Establecido esto, consideremos en el anillo $P = R[x]$ una sucesión débilmente creciente de ideales

$$(S) \quad \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots \subseteq \mathfrak{a}_p \subseteq \dots$$

y vamos a demostrar que a partir de un cierto lugar de orden todos los ideales de esta sucesión son iguales.

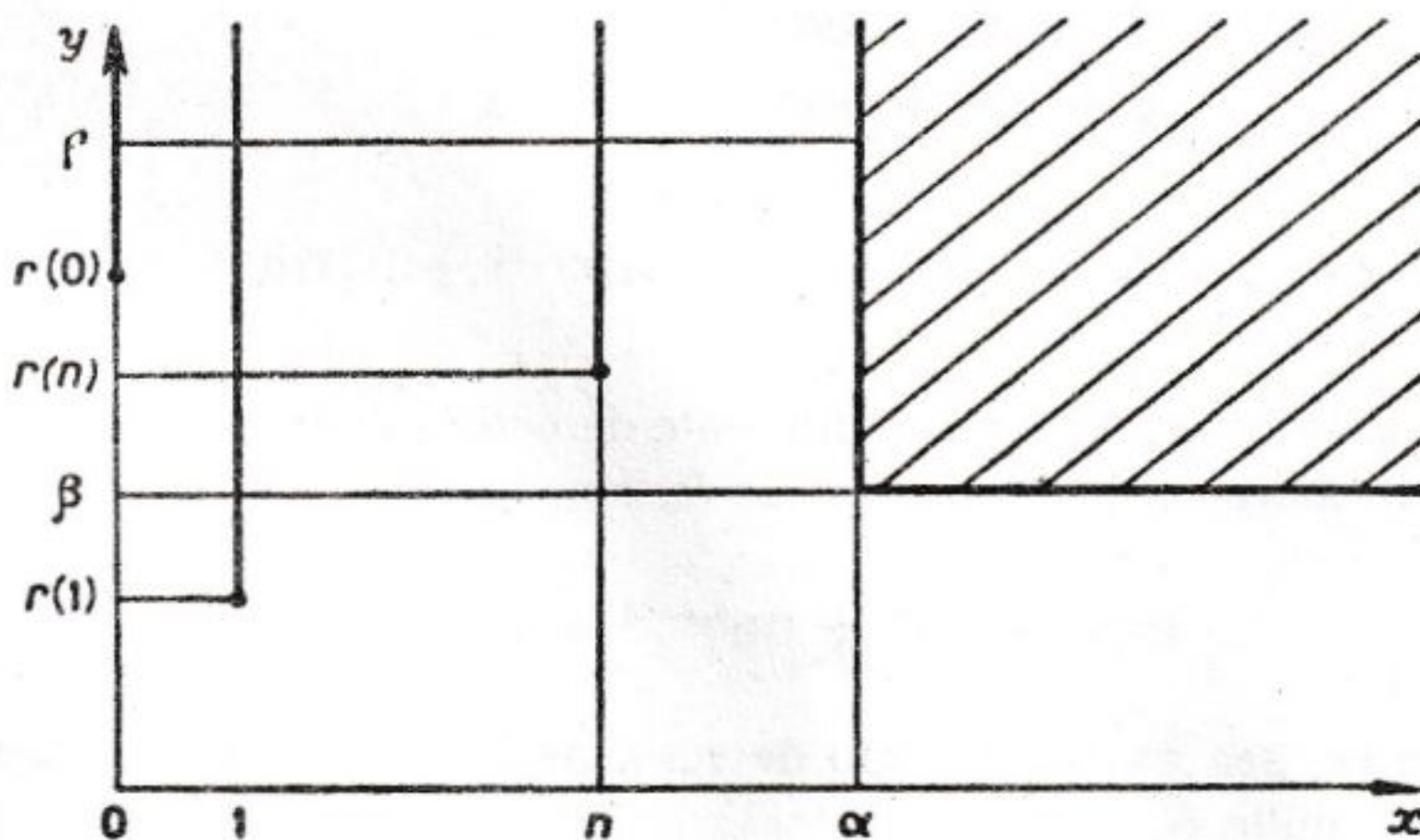
Para cada valor de n los ideales $C_n(\mathfrak{a}_p)$ forman también una sucesión débilmente creciente

$$C_n(\mathfrak{a}_1) \subseteq C_n(\mathfrak{a}_2) \subseteq \dots \subseteq C_n(\mathfrak{a}_p) \subseteq \dots$$

y puesto que el anillo noetheriano R verifica la condición de cadena ascendente, existe un entero $r = r(n)$, función de n , tal que

$$p \geq r \quad \text{implica} \quad C_n(\mathfrak{a}_p) = C_n(\mathfrak{a}_r).$$

Asociando a cada punto (n, p) de coordenadas enteras, en un plano xOy , el ideal $C_n(\mathfrak{a}_p)$, vemos que, sobre cada paralela al eje Oy de abscisa entera n , los ideales $C_n(\mathfrak{a}_p)$ van creciendo (débilmente) y son iguales entre sí sobre las semirrectas $p \geq r(n)$ (ver figura).



Se ve además, teniendo en cuenta el lema 1, que

$$(1) \quad n \leq h \quad y \quad p \leq k \quad \text{implican} \quad C_n(\mathfrak{a}_p) \leq C_h(\mathfrak{a}_k),$$

puesto que $C_n(\mathfrak{a}_p) \subseteq C_h(\mathfrak{a}_p) \subseteq C_h(\mathfrak{a}_k)$.

Pero como el anillo noetheriano R cumple la condición maximal, existe en el conjunto de ideales $C_n(\mathfrak{a}_p)$ un *ideal maximal* $C_\alpha(\mathfrak{a}_\beta)$, lo que, con la propiedad (1), implica que en el cuadrante $n \geq \alpha$, $p \geq \beta$, sombreado sobre la figura, todos los ideales $C_n(\mathfrak{a}_p)$ son iguales a $C_\alpha(\mathfrak{a}_\beta)$.

Sea entonces ρ el mayor de los enteros $r(1), \dots, r(\alpha - 1)$, β . Para todo n , la desigualdad $p \geq \rho$ implica

$$C_n(\mathfrak{a}_p) = C_n(\mathfrak{a}_\rho).$$

La igualdad $\mathfrak{a}_p = \mathfrak{a}_\rho$ para $p \geq \rho$ resulta según el lema siguiente.

Lema 2. — Si $\mathfrak{a}$ y $\mathfrak{b}$ son, en el anillo $P = R[x]$, dos ideales que cumplen las condiciones

$$\mathfrak{a} \subseteq \mathfrak{b} \quad y \quad C_n(\mathfrak{a}) = C_n(\mathfrak{b}) \quad \forall n \in N,$$

se tiene

$$\mathfrak{a} = \mathfrak{b}.$$

Puesto que $C_0(\mathfrak{a}) = C_0(\mathfrak{b})$, los ideales $\mathfrak{a}$ y $\mathfrak{b}$ contienen las mismas constantes, es decir los mismos polinomios de grado 0 (por supuesto, este conjunto de constantes comunes puede reducirse a $\{0\}$). Razonemos por recurrencia sobre el grado n de los polinomios, suponiendo que se ha establecido que, para todo $\nu \leq n - 1$; todo polinomio de grado ν perteneciente a $\mathfrak{b}$ pertenece también a $\mathfrak{a}$, y demostremos la misma propiedad para el grado n . La propiedad, establecida entonces para todo grado n , implicará la igualdad $\mathfrak{a} = \mathfrak{b}$.

Sea

$$g(x) = bx^n + b_1x^{n-1} + \dots \quad b \neq 0$$

un polinomio de $\mathfrak{b}$, de grado n . Tenemos

$$b \in C_n(\mathfrak{b}) = C_n(\mathfrak{a})$$

luego existe un polinomio de grado n ,

$$f(x) = bx^n + a_1x^{n-1} + \dots,$$

que pertenece a $\mathfrak{a}$, y tiene b como coeficiente director. El polinomio

$$f_1(x) = g(x) - f(x) = (b_1 - a_1)x^{n-1} + \dots$$

pertenece a $\mathfrak{b}$ y, si no es nulo, es de grado $\nu \leq n - 1$, luego pertenece a $\mathfrak{a}$, y lo mismo el polinomio $g = f + f_1$.

De paso en paso vemos, que si R es un anillo noetheriano con elemento unidad e el anillo $P_n = R[x_1, \dots, x_n]$ de los polinomios en $x_1, \dots, x_n$ con coeficientes de R es un anillo noetheriano. Tenemos en efecto

$$R[x_1, x_2] = R[x_1][x_2], \text{ etc...}$$

Un cuerpo K no tiene más ideales que los ideales principales (0) , (e) , luego todo cuerpo es un anillo noetheriano. El anillo de los enteros $\mathbf{Z}$, en el que todo ideal es principal (cap. IV, § 7) también es noetheriano. En consecuencia los anillos $K[x_1, \dots, x_n]$, $\mathbf{Z}[x_1, \dots, x_n]$ son noetherianos.

§ 3. Anillos principales

Un caso particular importante de anillos noetherianos es el que ofrecen los *anillos principales*.

Definición. — Se llama anillo principal al anillo conmutativo con elemento unidad en el que todo ideal es principal.

Hemos visto ya que esta propiedad se cumple en el anillo de los enteros, que es por ello un anillo principal.

Un segundo ejemplo nos lo da el teorema siguiente:

Teorema 1. — *Todo anillo euclídeo $\mathfrak{E}$ es principal.*

Sea en efecto $\mathfrak{a}$ un ideal de $\mathfrak{E}$. Si $\mathfrak{a} = (0)$, $\mathfrak{a}$ es ya un ideal principal. Sea pues $\mathfrak{a} \neq (0)$. Consideremos la función φ que interviene en la definición de un anillo euclídeo (cap. IV, § 6) y sea a uno de los elementos de $\mathfrak{a}$ para los cuales el entero $\varphi(a)$ es mínimo. Sea x un elemento de $\mathfrak{a}$. Por ser $\mathfrak{E}$ un anillo euclídeo, existen $q \in \mathfrak{E}$ y $r \in \mathfrak{E}$ tales que $x = aq + r$, con $r = 0$, ó $r \neq 0$ y $\varphi(r) < \varphi(a)$. Pero esta última circunstancia no puede darse por la elección de a y debe ser $r = 0$, luego $x = aq$, y $\mathfrak{a}$ es el ideal principal (a) .

Demos ahora las principales propiedades de los anillos principales sin divisores de cero.

Teorema 2. — *En un anillo principal sin divisores de cero, todo ideal primo es maximal.*

En efecto, sea $\mathfrak{p}$ un ideal primo. Si $\mathfrak{p}$ no es maximal, existirá un ideal propio $\mathfrak{a}$, que contenga a $\mathfrak{p}$ estrictamente. Pero $\mathfrak{p} = (p) \subset \mathfrak{a} = (a)$ implica $p = ra$, y, siendo la inclusión estricta, $a \notin \mathfrak{p}$, puesto que $a \in \mathfrak{p}$ implicaría entonces $\mathfrak{a} = \mathfrak{p}$; pero, siendo $\mathfrak{p}$ primo, resulta $r \in \mathfrak{p}$, es decir $r = r'p$. Las dos relaciones $p = ra$, $r = pr'$ implican entonces que r y p son asociados y $p = ra$, que a es una unidad, es decir que $\mathfrak{a}$ es el anillo completo, luego que $\mathfrak{p}$ es maximal.

En un anillo principal todo elemento es producto finito de elementos irreducibles. En efecto, sea a un elemento para el que no sucediese así. Se tendría entonces $a = a_1 b$, con uno al menos de los factores, sea a_1 , no igual a un producto finito de elementos irreducibles sin ser a_1 ni una unidad ni un asociado de a . Se tiene entonces, para a_1 , una descomposición análoga $a_1 = a_2 b_2$, con un factor a_2 , por ejemplo que no es producto finito de elementos irreducibles.

La sucesión de elementos $a_1, a_2, \dots$ puesta así en evidencia, en la que cada elemento divide a la anterior sin serle asociado ni ser una unidad, engendra una sucesión infinita estrictamente creciente de ideales principales

$$(a_1) \subset (a_2) \subset \dots$$

en contradicción con la condición de cadena ascendente que se cumple en todo anillo noetheriano, luego en particular en todo anillo principal.

De aquí vamos a deducir:

Teorema 3. — *Un anillo principal sin divisores de cero es un anillo factorial.*

Por ser todo elemento del anillo principal un producto finito de elementos irreducibles, sólo nos falta demostrar la unicidad de esta descomposición y nosotros sabemos (cap. IV, § 6) que es suficiente demostrar que si p es irreducible y divide a ab , divide a a ó a b (condición de Gauss).

Pero siendo el anillo principal, el ideal $(a) + (b)$ es principal. Luego existe un elemento d del anillo tal que

$$(a) + (b) = (d)$$

y en consecuencia dos elementos u y v del anillo tales que

$$d = au + bv;$$

pero por otra parte las inclusiones $(a) \subseteq (d)$ y $(b) \subseteq (d)$ implican que existan en el anillo elementos a' y b' tales que

$$a = a'd \quad b = b'd$$

de donde resulta que, en un anillo principal sin divisores de cero, dos elementos a y b admiten un máximo común divisor d dado por una expresión de la forma

$$d = au + bv.$$

En particular, en un anillo principal dos elementos a y p sin divisor común están ligados por una identidad de Bezout

$$1 = xa + yp.$$

Resulta, multiplicando por b , que si p divide a ab , divide también a b . De la demostración precedente resulta además que:

En un anillo principal —como en un anillo euclídeo— las tres propiedades I, II, III (cap. IV, § 6) son equivalentes para definir a los elementos primos entre sí.

Señalemos todavía que *en todo dominio de integridad que verifique la condición de Gauss —en particular, en todo anillo principal sin divisores de cero— el ideal (a) es primo si, y sólo si, a es irreducible.* En efecto, $xy \in (a)$, es decir $xy = pa$ implica si a es irreducible que a divide a uno de los factores, sea $x = ra$, es decir $x \in (a)$ y el ideal (a) es primo. Por el contrario, en todo anillo si a no es irreducible, (a) no es primo puesto que $a = pq$, donde p ó q no son unidades ni asociados a a es incompatible con $p = pa$ ó $q = p'a$. Se tiene pues $pq \in (a)$, $p \notin (a)$, $q \notin (a)$ y (a) no es primo.

§ 4. Propiedades de los ideales de un anillo noetheriano A

Teorema 1. — *Todo ideal primario $\mathfrak{q}$ de un anillo noetheriano A es primario fuerte, y por consiguiente, en un anillo noetheriano las dos nociones “primario” y “primario fuerte” coinciden.*

Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos ideales de A tales que se tenga $\mathfrak{ab} \subseteq \mathfrak{q}$, $\mathfrak{a} \not\subseteq \mathfrak{q}$. Existe un elemento a de $\mathfrak{a}$ que no pertenece a $\mathfrak{q}$. Si $(b_1, \dots, b_s)$ es una base del ideal $\mathfrak{b}$, las relaciones $a \notin \mathfrak{q}$, $ab_i \in \mathfrak{q}$ implica la existencia de enteros n_i tales que $b_i^{n_i} \in \mathfrak{q}$ ($i = 1, \dots, s$).

Una potencia $\mathfrak{b}^\lambda$ del ideal $\mathfrak{b}$ está engendrada por los productos $b_1^{\beta_1} \dots b_s^{\beta_s}$, con $\beta_1 + \dots + \beta_s = \lambda$, $\beta_i \geq 0$. Para

$$\lambda \geq 1 + (n_1 - 1) + \dots + (n_s - 1) = n_1 + \dots + n_s - (s - 1)$$

un β_i al menos es igual o mayor al n_i del mismo índice, lo que implica $b_i^{\beta_i} \in \mathfrak{q}$, $b_1^{\beta_1}, \dots, b_s^{\beta_s} \in \mathfrak{q}$ y finalmente $\mathfrak{b}^\lambda \subseteq \mathfrak{q}$.

Teorema 2. — *Dado un ideal $\mathfrak{m}$ en un anillo noetheriano A , existe un entero n tal que se tenga*

$$[\mathcal{R}(\mathfrak{m})]^n \subseteq \mathfrak{m}.$$

Sea $(r_1, \dots, r_s)$ una base de $\mathcal{R}(\mathfrak{m})$ y $n_1, \dots, n_s$ enteros tales que $r_i^{n_i} \in \mathfrak{m}$. El ideal $[\mathcal{R}(\mathfrak{m})]^n$ está engendrado por los productos $r_1^{\alpha_1} \dots r_s^{\alpha_s}$ donde $\alpha_1 + \dots + \alpha_s = n$, $\alpha_i \geq 0$. Si se toma, como en el teorema precedente

$$n \geq n_1 + \dots + n_s - (s - 1)$$

cada uno de los productos $r_1^{\alpha_1} \dots r_s^{\alpha_s}$ pertenece a $\mathfrak{m}$, y se tiene $[\mathcal{R}(\mathfrak{m})]^n \subseteq \mathfrak{m}$.

Corolario 1. — *Para todo ideal $\mathfrak{q}$ casi primario o primario de radical (primo) $\mathfrak{p}$, en un anillo noetheriano A , existe un mínimo entero ρ , llamado exponente de $\mathfrak{q}$, tal que se tiene*

$$\mathfrak{p}^\rho \subseteq \mathfrak{q} \subseteq \mathfrak{p}.$$

Corolario 2. — *Si $\mathfrak{p}$ es primo y si $\mathfrak{a}$ es un ideal verificando*

$$\mathfrak{p}^n \subseteq \mathfrak{a} \subseteq \mathfrak{p}$$

$\mathfrak{a}$ es casi primario de radical $\mathfrak{p}$.

Tenemos en efecto, de una parte, $\mathcal{R}(\mathfrak{p}^n) \subseteq \mathcal{R}(\mathfrak{a}) \subseteq \mathcal{R}(\mathfrak{p}) = \mathfrak{p}$, y de otra parte $\mathcal{R}(\mathfrak{p}^n) = \mathcal{R}(\mathfrak{p}) = \mathfrak{p}$ (cap. V, § 10, teor. 3, corol.), de donde $\mathcal{R}(\mathfrak{a}) = \mathfrak{p}$.

Si el anillo noetheriano A tiene elemento unidad e y si $\mathfrak{p}$ es maximal, un ideal $\mathfrak{a}$ con la condición

$$\mathfrak{p}^n \subseteq \mathfrak{a} \subseteq \mathfrak{p}$$

es $\mathfrak{p}$ -primario (cap. V, § 10, teor. 5); teniendo en cuenta el corolario 1 se deduce que en un anillo noetheriano con elemento unidad A , las potencias de un ideal $\mathfrak{p}$ -primario, donde $\mathfrak{p}$ es maximal, son $\mathfrak{p}$ -primarias.

Teorema 3. — *En un anillo noetheriano A , todo ideal irreducible es primario.*

Recordemos que un ideal $\mathfrak{i}$ es $\cap$ -irreducible o, más brevemente, irreducible, si no admite ninguna descomposición de la forma $\mathfrak{i} = \mathfrak{a} \cap \mathfrak{a}'$ con las inclusiones estrictas $\mathfrak{i} \subset \mathfrak{a}$, $\mathfrak{i} \subset \mathfrak{a}'$.

Para establecer este teorema mostraremos que si un ideal $\mathfrak{m}$ del anillo A no es primario, es reducible.

No siendo primario el ideal $\mathfrak{m}$ existirá al menos un par de elementos a, b de A verificando

$$ab \in \mathfrak{m}; \quad a \notin \mathfrak{m}; \quad \forall n \in \mathbb{N}, \quad b^n \notin \mathfrak{m}.$$

Designemos por $\mathfrak{m}_h$ el conjunto de elementos x del anillo tales que $xb^h \in \mathfrak{m}$; $\mathfrak{m}_h$ es un ideal, puesto que es el residual $\mathfrak{m} : \{b^h\} = \mathfrak{m} : (b^h)$.

En particular tenemos $a \in \mathfrak{m}_1$, de donde $\mathfrak{m} \subset \mathfrak{m}_1$ estrictamente puesto que $a \notin \mathfrak{m}$.

Según la definición de $\mathfrak{m}_h$, tenemos

$$\mathfrak{m}_h \subseteq \mathfrak{m}_{h+1}$$

y, por consiguiente, las $\mathfrak{m}_h$ forman una sucesión ilimitada, débilmente creciente. Puesto que el anillo A es noetheriano existe un entero k tal que

$$h \geq k \quad \text{implica} \quad \mathfrak{m}_h = \mathfrak{m}_k.$$

Consideremos el ideal Ab^k [conjunto de los elementos rb^k , $r \in A$; este ideal no coincide necesariamente con el ideal principal (b^k) porque no hemos supuesto la existencia de elemento unidad en A]. Pongamos

$$(1) \quad \mathfrak{m}' = \mathfrak{m} + Ab^k.$$

El ideal $\mathfrak{m}'$ contiene estrictamente a $\mathfrak{m}$, pues $b^{k+1} \in \mathfrak{m}'$ y $b^{k+1} \notin \mathfrak{m}$.

Habremos, pues, mostrado que $\mathfrak{m}$ es reducible si establecemos la igualdad

$$\mathfrak{m} = \mathfrak{m}_1 \cap \mathfrak{m}'.$$

Puesto que $\mathfrak{m}$ está contenido en $\mathfrak{m}_1$ y en $\mathfrak{m}'$, tendremos $\mathfrak{m} \subseteq \mathfrak{m}_1 \cap \mathfrak{m}'$. Recíprocamente, sea $x \in \mathfrak{m}_1 \cap \mathfrak{m}'$. Según (1) podemos escribir

$$x = m + rb^k \quad \text{donde} \quad m \in \mathfrak{m}, r \in A,$$

lo que implica, puesto que $x \in \mathfrak{m}_1$,

$$bx = bm + rb^{k+1} \in \mathfrak{m}$$

luego $rb^{k+1} \in \mathfrak{m}$, $r \in \mathfrak{m}_{k+1}$ y, puesto que $\mathfrak{m}_{k+1} = \mathfrak{m}_k$, $rb^k \in \mathfrak{m}$, luego $x \in \mathfrak{m}$. Tenemos, pues, $\mathfrak{m}_1 \cap \mathfrak{m}' \subseteq \mathfrak{m}$, de donde la igualdad, y $\mathfrak{m}$ es reducible, c.q.d.

§ 5. Descomposición noetheriana

Hemos visto (cap. VI, § 2, teor. 4) que, en un anillo cualquiera todo ideal es intersección de los ideales irreducibles que le contienen.

Vamos a obtener ahora, en el caso de un anillo noetheriano (seguimos sobre-

entendiendo que conmutativo), propiedades más precisas.

Teorema 1. — *En un anillo noetheriano A , todo ideal $\mathfrak{m}$ es la intersección de un número finito de ideales irreducibles:*

$$\mathfrak{m} = \mathfrak{i}_1 \cap \dots \cap \mathfrak{i}_r \quad (r \geq 1).$$

Supongamos que existe en A un ideal $\mathfrak{m}$ que no sea como afirma el teorema. En particular, $\mathfrak{m}$ no será irreducible; existirán, pues, dos ideales $\mathfrak{m}_1$ y $\mathfrak{m}'_1$ tales que se tenga

$$\mathfrak{m} = \mathfrak{m}_1 \cap \mathfrak{m}'_1, \quad \mathfrak{m} \subset \mathfrak{m}_1, \quad \mathfrak{m} \subset \mathfrak{m}'_1$$

(estrictamente). Uno al menos de los dos ideales $\mathfrak{m}_1, \mathfrak{m}'_1$ no será intersección finita de ideales irreducibles: sea así para $\mathfrak{m}_1$.

En particular, $\mathfrak{m}_1$ no es irreducible. Existen, pues, dos ideales $\mathfrak{m}_2$ y $\mathfrak{m}'_2$ tales que

$$\mathfrak{m}_1 = \mathfrak{m}_2 \cap \mathfrak{m}'_2, \quad \mathfrak{m}_1 \subset \mathfrak{m}_2, \quad \mathfrak{m}_1 \subset \mathfrak{m}'_2$$

(estrictamente) y uno de los dos, digamos $\mathfrak{m}_2$, no es intersección de ideales irreducibles. Reiterando el razonamiento se obtiene una sucesión estrictamente creciente indefinida

$$\mathfrak{m} \subset \mathfrak{m}_1 \subset \mathfrak{m}_2 \subset \dots$$

lo que es imposible, puesto que el anillo A verifica la condición de cadena ascendente.

Entre los ideales irreducibles de un anillo conmutativo cualquiera encontramos, evidentemente, los *ideales maximales*; también tenemos a los ideales primos, pues si se tiene

$$\mathfrak{p} = \mathfrak{m}_1 \cap \mathfrak{m}_2$$

luego

$$\mathfrak{m}_1 \mathfrak{m}_2 \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 = \mathfrak{p} \subseteq \mathfrak{m}_i \quad (i = 1, 2)$$

resulta, siendo $\mathfrak{p}$ primo, que uno al menos de los ideales $\mathfrak{m}_i$ está contenido en $\mathfrak{p}$, luego es igual a $\mathfrak{p}$; $\mathfrak{p}$ es efectivamente irreducible. Finalmente, hemos visto que en un anillo noetheriano todo ideal irreducible es primario. Naturalmente, la recíproca de este teorema no es cierta; existen ideales primarios que no son irreducibles, por ejemplo todas las intersecciones normadas de un número finito

$n (> 1)$ de ideales primarios con el mismo radical.

Relacionando los teoremas 1 y 3 del § 4, podemos enunciar:

Teorema 2 (Emmy Noether) ¹. — *En un anillo noetheriano A , todo ideal es la intersección de un número finito de ideales primarios.*

Reemplazando los ideales primarios de igual radical por su intersección, y suprimiendo en la intersección los componentes superfluos, se obtiene una intersección normada de ideales primarios y utilizando los teoremas 5 y 6 (capítulo V, § 11) se puede enunciar:

En un anillo noetheriano A , todo ideal *puede representarse* como intersección finita normada de ideales primarios y todas estas representaciones tienen *el mismo número de componentes primarios; los radicales de estos componentes, o "ideales primos esenciales" están unívocamente determinados, así como todos los componentes aislados.*

Además, se puede asociar a todo ideal $\mathfrak{a}$, una entre sus representaciones como intersección de ideales primarios, caracterizada por la siguiente propiedad.

Los ideales primarios —no unívocamente determinados—, se eligen de exponente mínimo, y ellos mismos mínimos entre los que tienen la misma propiedad.

Esto es posible, pues si $\mathfrak{p}_i$ es un ideal primo maximal en el conjunto $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$,

$$\mathfrak{b}_i = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \dots \cap \mathfrak{q}_r$$

es un componente aislado, luego determinado unívocamente. Entre los $\mathfrak{q}_i$ de radical $\mathfrak{p}_i$ tales que $\mathfrak{a} = \mathfrak{q}_i \cap \mathfrak{b}_i$, se elige uno $\bar{\mathfrak{q}}_i$, de exponente mínimo, y se recommienza sobre $\mathfrak{b}_i$ el mismo razonamiento.

Si se toma entonces la intersección de todas las representaciones posibles de ese tipo, se obtiene la representación buscada, puesto que la intersección de una familia *cualquiera* de ideales primarios *del mismo radical y del mismo exponente* es un ideal primario del mismo radical y del mismo exponente (observación al teor. 6 de cap. V, § 10).

¹ El teorema fue demostrado primero para el caso de anillos de polinomios por el gran ajedrecista Lasker, que introdujo la noción de ideal primario. A Emmy Noether se debe el haber descubierto que el teorema es consecuencia de la condición de cadena ascendente. (N. del T., según Zariski-Samuel.)

CAPÍTULO VIII

COMPLEMENTOS DE LA TEORIA DE LOS GRUPOS

§ 1. Grupos con operadores

Hemos definido (cap. II, § 6) un *grupo con operadores* como un grupo G al que está asociado un conjunto $\Delta = \{\alpha, \beta, \dots\}$ de elementos $\alpha, \beta, \dots$ llamados *operadores*, con una *ley de composición externa* que aplica $\Delta \times G$ en G , y es *distributiva respecto a la ley de composición interna de G* . Utilizando el signo $*$ para la ley de composición externa, y $\top$ para la interna, lo anterior se formula:

$$(1) \quad \alpha * (x \top y) = (\alpha * x) \top (\alpha * y), \quad \forall x, y \in G \quad \text{y} \quad \forall \alpha \in \Delta;$$

cuando se usa notación multiplicativa para las dos leyes la formulación es:

$$(1) \quad \alpha(xy) = (\alpha x)(\alpha y), \quad \forall x, y \in G \quad \text{y} \quad \forall \alpha \in \Delta;$$

y, finalmente, utilizando notación multiplicativa para la ley externa y aditiva para la interna:

$$(1) \quad \alpha(x + y) = \alpha x + \alpha y, \quad \forall x, y \in G \quad \text{y} \quad \forall \alpha \in \Delta.$$

Por comodidad llamaremos Δ -grupo a un grupo cuyo dominio de operadores es Δ . Un Δ -grupo es también un Δ' -grupo si Δ' es un subconjunto cualquiera de Δ .

La distributividad (1) significa que, siendo α un elemento de Δ , la aplicación $x \rightarrow \alpha x$ de G en sí mismo es un *endomorfismo* $\bar{\alpha}$ de G (desde luego, elementos distintos $\alpha, \alpha_1, \dots$ de Δ pueden dar lugar al mismo endomorfismo $\bar{\alpha}$,

como hemos visto más generalmente en el cap. II, § 6, a propósito de la reducción de un dominio de operadores).

La condición (1) implica pues, llamando e al elemento neutro de G , $ae = \bar{a}e = e$, porque en cualquier endomorfismo la imagen de e es el mismo e .

Por razón análoga tenemos $a(x^{-1}) = (ax)^{-1}$.

Estas propiedades conducen a considerar, para un grupo G , algunos dominios de operadores especialmente importantes:

- a) el conjunto Δ_1 de todos los endomorfismos de G ;
- b) el conjunto Δ_2 de todos los automorfismos de G ;
- c) el conjunto Δ_3 de los automorfismos internos de G ;
- d) el conjunto $\Delta_4 = \{\epsilon\}$ que sólo comprende al automorfismo idéntico (o identidad) $\epsilon(\epsilon x = x, \forall x \in G)$. Si G es abeliano $\Delta_3 = \Delta_4$.

Desde luego, el caso d) es banal, pero su interés, como luego veremos con precisión, está en que permite ver todas las propiedades de los grupos ordinarios como casos particulares de las de los grupos con operadores.

En el dominio de operadores Δ pueden tenerse también leyes de composición; entonces, éstas vienen sujetas ordinariamente a condiciones suplementarias. En este orden de ideas los dos tipos de estructura más importantes son los *módulos* sobre un anillo A , o A -módulos, y los *espacios vectoriales* sobre un cuerpo K .

Dado un anillo A se llama A -módulo (a la izquierda) un grupo abeliano M (aditivo, es decir, con su ley de composición interna en notación aditiva) que tiene a A como dominio de operadores, lo que implica la condición

$$(1) \quad a(x + y) = ax + ay \quad \forall x, y \in M \quad \text{y} \quad \forall a \in A,$$

y con las dos condiciones suplementarias siguientes:

$$(2) \quad (a + \beta)x = ax + \beta x \quad \forall x \in M \quad \text{y} \quad \forall a, \beta \in A$$

(distributividad a la izquierda), y

$$(3) \quad a(\beta x) = (a\beta)x \quad \forall x \in M \quad \text{y} \quad \forall a, \beta \in A$$

(asociatividad mixta). Un A -módulo se llama *unitario* cuando A tiene un elemento unidad ϵ y este es operador unidad (o idéntico):

$$(4) \quad \epsilon x = x \quad \forall x \in M.$$

Todo superanillo B de A es un A -módulo donde la ley externa coincide

con la multiplicación en B ; todo ideal a la izquierda $\mathfrak{m}$ de un anillo A es un A -módulo (a la izquierda) donde el producto ax ($a \in A, x \in \mathfrak{m}$) es el producto ordinario en A ; por ser $\mathfrak{m}$ ideal a la izquierda, ax es elemento de $\mathfrak{m}$, lo que da efectivamente una ley de composición externa que aplica $A \times \mathfrak{m}$ en $\mathfrak{m}$, cumpliéndose las condiciones (1), (2), (3); y también la (4) si en A , hay elemento unidad. Finalmente mencionemos que todo grupo abeliano G es un $\mathbb{Z}$ -módulo sobre el anillo $\mathbb{Z}$ de los enteros.

Si se reemplaza la condición (3) por la condición

$$(3') \quad a(\beta x) = (\beta a)x$$

no se define un A -módulo a la izquierda, sino un A -módulo a la derecha; entonces es más cómodo considerar la ley externa como una aplicación de $M \times A$ en M y, en consecuencia, escribir los operadores a la derecha; la condición (3') se expresa entonces

$$(3'') \quad (x\beta)a = x(\beta a),$$

y las condiciones (1) y (2), respectivamente,

$$(1'') \quad (x + y)a = xa + ya,$$

$$(2'') \quad x(\alpha + \beta) = x\alpha + x\beta.$$

Cuando el anillo A es conmutativo no ha lugar a distinguir entre A -módulos a la derecha y a la izquierda.

Se llama *espacio vectorial a la izquierda* (por ejemplo) sobre un cuerpo K un K -módulo a la izquierda unitario.

Todo supercuerpo L de K es un espacio vectorial a la izquierda sobre K , cuya ley externa coincide con el producto en L .

Dado un cuerpo K consideremos el conjunto V de entes

$$v = (x_1, \dots, x_n) \quad (x_i \in K)$$

donde n es un entero fijo, y les llamaremos *vectores de n coordenadas* sobre el cuerpo K , definiendo

$$(x_1, \dots, x_n) = (y_1, \dots, y_n) \quad \text{si} \quad x_i = y_i \quad (i = 1, \dots, n).$$

Definiremos luego una adición en V , poniendo

lo que hace de V un *grupo aditivo*; finalmente introduciremos una ley de composición externa aplicando $K \times V$ en V , poniendo, para todo a de K ,

$$a(x_1, \dots, x_n) = (ax_1, \dots, ax_n)$$

Entonces V es un *grupo con operadores*, cuyo dominio de operadores es el cuerpo K (los elementos de K se llaman escalares cuando se le mira como operadores sobre los vectores de V). Junto con (1) se tienen las igualdades (2), (3) y (4), y V es un espacio vectorial a la izquierda sobre el cuerpo K .

El conjunto $\mathcal{F}$ de las funciones reales definidas sobre el cuerpo $\mathbf{R}$ de los números reales, con las reglas de cálculo clásicas, es un espacio vectorial sobre $\mathbf{R}$.

Para todo espacio vectorial V sobre un cuerpo K , según las fórmulas fundamentales (1), (2), (3), (4), valen las siguientes reglas de cálculo, en las que hemos puesto 0 para el cero del cuerpo K y $\bar{0}$ para el cero del grupo aditivo V :

$$0v = \bar{0} \quad \forall v \in V$$

porque $av + \bar{0} = av = (a + 0)v = av + 0v \quad (a \in K);$

$$a\bar{0} = \bar{0} \quad \forall a \in K$$

(como ya hemos visto); además $av = \bar{0}$ y $a \neq 0$ implican

$$a^{-1}(av) = a^{-1}\bar{0} = \bar{0} \quad \text{es decir} \quad (a^{-1}a)v = \epsilon v = v = \bar{0}$$

Se llama *álgebra asociativa* (o *sistema hipercomplejo*) sobre un cuerpo K un espacio vectorial sobre K que tiene, además, la propiedad de ser un anillo. Por ejemplo, el conjunto $\mathbf{C}$ de los complejos es un álgebra asociativa sobre el cuerpo de los reales.

Sea G un grupo con operadores y Δ el dominio de éstos. Un subgrupo H de G se dice *lícito* o *permitido* respecto al dominio de operadores Δ (o *estable* para la correspondiente ley de composición externa, o *compatible* con ella) si

cualesquiera sean $a \in \Delta$ y $h \in H$, se tiene $ah \in H$.

Diremos entonces, más brevemente, que H es un Δ -subgrupo de G . Si Δ' es un subconjunto de Δ , todo Δ -subgrupo es un Δ' -subgrupo.

Ejemplos. — 1. El subgrupo $E = (e)$ formado por el elemento neutro es Δ -subgrupo para todo dominio de operadores Δ .

2. a) Si Δ es el conjunto Δ_1 de endomorfismos del grupo considerado G , los Δ -subgrupos son, por definición, los *subgrupos completamente invariantes*.

b) Si Δ es el conjunto Δ_2 de todos los automorfismos de G los Δ -subgrupos son, por definición, los *subgrupos característicos* de G .

c) Si Δ es el conjunto Δ_3 de los automorfismos internos de G , los Δ -subgrupos son los *subgrupos distinguidos* (o invariantes o normales).

d) Si Δ se reduce al operador idéntico ϵ , todos los subgrupos de G son lícitos.

Todo subgrupo completamente invariante es característico, todo subgrupo característico es distinguido.

Con un dominio de operadores cualquiera Δ , los subgrupos que desempeñan un papel más importante son los subgrupos distinguidos y lícitos, o Δ -subgrupos distinguidos.

3. Sea A un anillo conmutativo considerado como grupo aditivo. El mismo A va a ser el dominio de operadores, con su multiplicación como ley externa. Los subgrupos permitidos son los ideales del anillo A . Las proposiciones sobre grupos con operadores se aplican pues inmediatamente en teoría de ideales.

4. Siendo A un anillo y M un A -módulo, a la izquierda por ejemplo, se ve inmediatamente que un subgrupo permitido H de M es él mismo un A -módulo a la izquierda. Por este motivo, los subgrupos permitidos de un módulo se llaman *submódulos*. En particular, un subgrupo permitido de un espacio vectorial es él mismo un espacio vectorial sobre K , al que se da el nombre de *subespacio*.

Teorema 1. — *Los Δ -subgrupos de un Δ -grupo G forman una familia de Moore que es $\mathbf{U}$ -inductiva.*

Para que un subgrupo de G sea un Δ -subgrupo, es necesario y suficiente que sea estable para la familia $\bar{\Delta}$ de los endomorfismos $\bar{\alpha}$, ... asociados a los operadores α , ... de Δ . La familia de los Δ -subgrupos es pues, la intersección de la familia de Moore de los subgrupos y de la familia de Moore de las partes estables para la familia de aplicaciones $\bar{\Delta}$; y se sabe que la intersección de dos familias de Moore es una familia de Moore.

Además, por ser $\mathbf{U}$ -inductiva la familia de Moore de los subgrupos de G (cap. VI, § 1), lo es igualmente la familia de los Δ -subgrupos, pues, siendo C una cadena de tales subgrupos S , el subgrupo $R = \bigcup_{S \in C} S$ es permitido (si

$r \in R$, se tiene por lo menos un $S \in \mathcal{C}$, $r \in S$ de donde para todo $\alpha \in \Delta$, $\alpha r \in S \subseteq R$).

Del teorema anterior resulta que los Δ -subgrupos del Δ -grupo G forman un *retículo completo* en el que el ínfimo coincide con la intersección conjuntista. El supremo de este retículo no es otro que la unión completa, como demuestra el siguiente teorema.

Teorema 2. — *La unión completa R de una familia $\mathcal{F}$ de Δ -subgrupos de G , es un Δ -subgrupo.*

R es el conjunto de productos finitos

$$r = x_1 \dots x_k$$

formados con elementos x_i tomados en los grupos H de la familia $\mathcal{F}$. Ahora bien, para todo operador $\alpha \in \Delta$, tenemos, según (1) (extendido por una recurrencia inmediata a cualquier número de factores)

$$\alpha r = (\alpha x_1) \dots (\alpha x_k)$$

donde $\alpha x_i \in H_i$; luego $\alpha r \in R$, c.q.d.

Corolario. — *El retículo de los Δ -subgrupos es un subretículo del retículo de los subgrupos.*

Cuando G es un grupo *abeliano* escrito aditivamente, la unión completa se traduce en la suma. Lo que precede lleva consigo la definición de *submódulo suma de una familia de submódulos*, y la de *subespacio suma de una familia de subespacios vectoriales*.

Teniendo en cuenta el teorema precedente, del hecho de que el retículo de los subgrupos de un grupo abeliano es modular, y de que todo subretículo de un retículo modular es modular, resulta que *el retículo de los submódulos de un módulo, y el retículo de los subespacios de un espacio vectorial, son modulares*.

Observación. — *El retículo de los subespacios de un espacio vectorial $\mathcal{E}$ no es en general distributivo.* Tomemos en efecto para $\mathcal{E}$ el conjunto de los vectores libres del plano (por ejemplo sobre el cuerpo real $\mathbf{R}$) y consideremos los tres subespacios X, Y, Z formados por los vectores paralelos respectivamente a tres direcciones distintas. Tenemos.

$$X + (Y \cap Z) = X + 0 = X$$

y

$$X + Y = \mathcal{E}, \quad X + Z = \mathcal{E}$$

luego

$$(X + Y) \cap (X + Z) = \varepsilon \cap \varepsilon = \varepsilon.$$

La inclusión

$$X + (Y \cap Z) \subset (X + Y) \cap (X + Z)$$

es estricta.

Definiciones. — En un Δ -grupo G diremos que una relación de equivalencia $\mathcal{R}$ es *lícita o permitida* respecto a Δ (o compatible con Δ) o que $\mathcal{R}$ es una Δ -equivalencia si

$$(5) \quad x \equiv y (\mathcal{R}) \quad \text{implica} \quad \forall \alpha \in \Delta \quad \alpha x \equiv \alpha y (\mathcal{R})$$

Diremos que un homomorfismo h que aplica un Δ -grupo G sobre un Δ -grupo $\bar{G}$ es *lícito o permitido* para Δ (o compatible con Δ) o que es un Δ -homomorfismo si se tiene.

$$(6) \quad h(\alpha x) = \alpha(hx) \quad \forall x \in G \quad y \quad \forall \alpha \in \Delta.$$

Esta propiedad expresa en suma que h es permutable con cualquier operador α del dominio Δ . Esto se aplica en particular a los isomorfismos.

Teorema 3. — 1.º El homomorfismo canónico asociado a una Δ -equivalencia $\mathcal{R}$ es un Δ -homomorfismo.

2.º Si h es un Δ -homomorfismo, la equivalencia de homomorfismo $\mathcal{K}$ es una Δ -equivalencia.

3.º Si S es un Δ -subgrupo de G , las equivalencias $\mathcal{R}'_S, \mathcal{R}''_S$ que descomponen a G en clases a la derecha y en clases a la izquierda respecto a S , son Δ -equivalencias; además, si S es distinguido, el homomorfismo canónico $G \sim G/S$ es un Δ -homomorfismo.

1.º Sea $X \in G/\mathcal{R}$ una clase módulo $\mathcal{R}$; para dos elementos x, x_1 de X tenemos

$$x \equiv x_1 (\mathcal{R}) \quad \text{de donde} \quad \alpha x \equiv \alpha x_1 (\mathcal{R}).$$

La clase que contiene a αx , para $x \in X$ es, pues, independiente de la elección de x en X . Designaremos a esa clase por αX , definiendo así una ley externa aplicación de $\Delta \times (G/\mathcal{R})$ en $G/\mathcal{R}$.

Con esto, el homomorfismo canónico γ está definido por $\gamma x = X$ si $x \in X$. Como, por lo que precede, tenemos

$$\alpha X = \gamma(\alpha x), \quad \text{es decir} \quad \alpha(\gamma x) = \gamma(\alpha x)$$

para todo $a \in \Delta$, γ es un Δ -homomorfismo.

2.º Sea $x \equiv y(\mathcal{K})$, es decir, $h(x) = h(y)$. Resulta $a \cdot h(x) = a \cdot h(y)$ para todo $a \in \Delta$, de donde, siendo h permitido $h(ax) = h(ay)$, es decir $ax \equiv ay(\mathcal{K})$.

3.º Sea $a \equiv b(\mathcal{R}'_S)$, es decir $ba^{-1} = s \in S$; como S es un Δ -subgrupo resulta

$$a(ba^{-1}) = ab \cdot (aa)^{-1} = as \in S, \quad \forall a \in \Delta$$

luego $aa \equiv ab(\mathcal{R}'_S)$; así vemos que $\mathcal{R}'_S$ es una Δ -equivalencia, y del mismo modo se ve para $\mathcal{R}''_S$.

Si S es distinguido, tenemos $\mathcal{R}'_S = \mathcal{R}''_S$ y esta equivalencia compatible con la ley interna de G es la equivalencia de homomorfismo para el canónico $G \sim G/S$. Este homomorfismo canónico es pues, según la primera parte, un Δ -homomorfismo.

Teorema 4. — (*Teorema de homomorfismo para los Δ -grupos*). En un Δ -homomorfismo

$$(h) \quad G \sim \bar{G} = h(G)$$

que aplica un Δ -grupo G sobre un Δ -grupo $\bar{G}$, el núcleo N es un Δ -subgrupo (distinguido) y el isomorfismo

$$\bar{G} \simeq G/N$$

es un Δ -isomorfismo.

Cualesquiera sean $n \in N$ y $a \in \Delta$, tenemos, siendo $\bar{e}$ el elemento unidad de $\bar{G}$:

$$a \cdot h(n) = a\bar{e} = \bar{e}$$

luego, puesto que h es un Δ -isomorfismo

$$h(an) = a \cdot h(n) = \bar{e}$$

y, por consiguiente, $an \in N$; N es un Δ -subgrupo, c.q.d.

En el isomorfismo i un elemento $\bar{x}$ de $\bar{G}$ tiene por imagen la clase $X = i(\bar{x})$ conjunto de los elementos x de G tales que $h(x) = \bar{x}$. Para hacer de G/N un Δ -grupo, hemos definido aX como la clase que contiene a ax . Puesto que $h(ax) = a \cdot h(x) = a\bar{x}$, la clase aX es, en el isomorfismo i , la imagen de $a\bar{x}$; i es un Δ -isomorfismo, c.q.d.

Dado el Δ -homomorfismo

$$G \sim \bar{G} = h(G)$$

consideremos, según el *primer teorema de isomorfismo* (cap. II, § 5) la biyección entre los subgrupos $\bar{S}$ de $\bar{G}$ y los subgrupos S de G que contienen al núcleo N del homomorfismo h . Como sabemos, si S es subgrupo distinguido de G , su imagen $h(S)$ es subgrupo distinguido de $\bar{G}$, y si $\bar{S}$ es subgrupo distinguido de $\bar{G}$, su imagen recíproca $h^{-1}(\bar{S})$ es subgrupo distinguido de G .

Teorema 5. — 1.º Si S es un Δ -subgrupo de G , su imagen $h(S)$ es un Δ -subgrupo de $\bar{G}$; si $\bar{S}$ es un Δ -subgrupo de $\bar{G}$, su imagen recíproca $h^{-1}(\bar{S})$ es un Δ -subgrupo de G .

2.º Si $\bar{S}$ y $h^{-1}(\bar{S}) = S$ son Δ -subgrupos distinguidos (respectivamente de G y $\bar{G}$), los isomorfismos

$$\bar{G}/\bar{S} \simeq G/S \simeq (G/N)/(S/N)$$

son Δ -isomorfismos.

1.º Sea $\bar{x} = h(s)$ donde $s \in S$; tenemos

$$a\bar{x} = ah(s) = h(as) \quad \text{donde} \quad as \in S$$

luego $a\bar{x} \in h(S)$; $h(S)$ es un Δ -subgrupo de $\bar{G}$.

Sea x un elemento de $h^{-1}(\bar{S})$: $h(x) = \bar{s} \in \bar{S}$. Tenemos

$$h(ax) = ah(x) = a\bar{s} \in \bar{S}$$

luego $ax \in h^{-1}(\bar{S})$ y $h^{-1}(\bar{S})$ es, en efecto, un Δ -subgrupo de G .

2.º El isomorfismo

$$(j) \quad \bar{G}/\bar{S} \simeq G/S$$

se ha definido, como recordaremos, del siguiente modo:

$$X = Sx = j(\bar{X}) \quad \text{si} \quad \bar{X} = \bar{S}\bar{x} \quad \text{con} \quad \bar{x} = h(x).$$

Como $aX = S(ax)$, $a\bar{X} = \bar{S}(a\bar{x})$ y $a\bar{x} = ah(x) = h(ax)$, tenemos en efecto

$$\text{y } j \text{ es un } \Delta\text{-isomorfismo.} \quad aX = j(a\bar{X}) \quad \forall a \in \Delta$$

El isomorfismo

$$(j_1) \quad G/S \simeq (G/N)/(S/N)$$

está definido por

$$j_1(X) = (S/N)X \quad \text{si} \quad X = Sx (\in G/S) \quad \text{y} \quad X_1 = Nx (\in G/N)$$

Pero entonces tenemos $\alpha X = S(\alpha x)$, $\alpha X_1 = N(\alpha x)$, luego $j_1(\alpha X) = \alpha X_1$.

§ 2. Segundo teorema de isomorfismo

Lema 1. — Si H y K son dos subgrupos de un grupo G y si S es un subgrupo distinguido de H , $S \cap K$ es subgrupo distinguido de $H \cap K$.

En efecto, para todo elemento x de $S \cap K$ y todo elemento m de $H \cap K$, $m x m^{-1}$ pertenece de una parte a S (porque $m \in H$ y $x \in S$ subgrupo distinguido de H) y de otra parte a K (porque $m \in K$ y $x \in K$).

Lema 2. — Si G_1, G_2 , son dos subgrupos de un grupo G , el complejo producto

$$G_1 G_2 = \{ g_1 g_2 ; g_1 \in G_1, g_2 \in G_2 \}$$

es un subgrupo de G si y sólo si G_1 y G_2 son permutables (es decir, si $G_1 G_2 = G_2 G_1$).

Si $G_1 G_2$ es un subgrupo P , tendremos designando por X —el conjunto de los inversos de los elementos de X (cap. II, § 4):

$$G_1 G_2 = P = P^- = G_2^- G_1^- = G_2 G_1.$$

Recíprocamente, si G_1 y G_2 son permutables, su unión completa coincide con el producto $G_1 G_2$ (cap. III, § 1), luego el producto es un grupo.

Lema 3.— Si G_1, G_2 son dos subgrupos permutables de un grupo G , G_1 es distinguido en $G_1 G_2$ si, y sólo si, G_1 es permutable con cada elemento de G_2 . Cuando es así, $G_1 \cap G_2$ es subgrupo distinguido de G_2 .

Si G_1 es distinguido en el grupo producto $G_1 G_2$, es, por definición, permutable con todo elemento de $G_1 G_2$, en particular con todo elemento de G_2 .

Recíprocamente, si G_1 es permutable con cada elemento g_2 de G_2 tenemos

$$\forall g_1 \in G_1 \quad \text{y} \quad \forall g_2 \in G_2, \quad g_1 g_2 G_1 = g_1 G_1 g_2 = G_1 g_2 = G_1 g_1 g_2$$

y G_1 es distinguido en $G_1 G_2$.

Según el lema 1, $G_1 \cap G_2$ es subgrupo distinguido $G_1 G_2 \cap G_2 = G_2$.

Suponiendo siempre G_1 permutable con cada elemento de G_2 , consideremos, teniendo en cuenta el lema 3, los grupos cocientes G_1G_2/G_1 , y $G_2/G_1 \cap G_2$.

Toda clase $X \in G_1G_2/G_1$ es de la forma

$$X = g_1g_2G_1 = G_1g_1g_2 = G_1g_2 = g_2G_1 \quad (g_i \in G_i).$$

En ella está el elemento g_2 de G_2 ; su intersección con G_2 es el conjunto de los elementos g'_2 de G_2 situados en la misma clase a la izquierda respecto a G_1 :

$$g'_2G_1 = g_2G_1 \quad \text{es decir} \quad g_2^{-1}g'_2 \in G_1.$$

Ahora, esta última relación equivale a

$$g_2^{-1}g'_2 \in G_1 \cap G_2 \quad \text{o} \quad g'_2 \in g_2(G_1 \cap G_2),$$

que expresa que g'_2 pertenece a la clase $Y \in G_2/G_1 \cap G_2$ que contiene a g_2 . Se tiene pues

$$X \cap G_2 = g_2(G_1 \cap G_2) = Y$$

Recíprocamente, toda clase $Y = g_2(G_1 \cap G_2) \in G_2/G_1 \cap G_2$ está contenida en la clase $X = g_2G_1 = YG_1 \in G_1G_2/G_1$.

Según lo que precede, para un elemento X de G_1G_2/G_1 y un elemento Y de $G_2/G_1 \cap G_2$, son equivalentes las cuatro propiedades siguientes:

$$X \text{ e } Y \text{ tienen un elemento común } g_2 \text{ de } G_2,$$

$$X \cap G_2 = Y, \quad X \supseteq Y, \quad X = YG_1,$$

y cualquiera de las cuatro define una biyección

$$X \xrightarrow{\beta} Y = X \cap G_2$$

que aplica el grupo cociente G_1G_2/G_1 sobre el grupo cociente $G_2/G_1 \cap G_2$.

Las clases X se multiplican como sus representantes g_2 , y lo mismo sucede con las clases Y : la biyección β es pues un isomorfismo entre G_1G_2/G_1 y $G_2/G_1 \cap G_2$. Podemos enunciar:

Teorema (segundo teorema de isomorfismo). — Si en un grupo G , un subgrupo G_1 es permutable con cada elemento de un subgrupo G_2 , G_1G_2 es un subgrupo que contiene a G_1 como subgrupo distinguido, $G_1 \cap G_2$ es subgrupo distinguido de G_2 , y los dos grupos cocientes G_1G_2/G_1 y $G_2/G_1 \cap G_2$ son isomorfos.

$$G_1G_2/G_1 \simeq G_2/(G_1 \cap G_2).$$

Observación. — Las hipótesis del teorema se cumplen, en particular cuando G_1 es subgrupo distinguido de G , siendo G_2 un subgrupo cualquiera.

Aplicaciones. — 1.º Sea G un grupo de orden finito: $O(G) = mp^r$, donde p es primo y no divisor de m : si S es un subgrupo de G de orden p^r (p -subgrupo de Sylow), todo elemento x de G de orden p^v ($0 \leq v < r$) que sea permutable con S , pertenece a S .

La hipótesis $xS = Sx$ implica, para todo entero α , $x^\alpha S = Sx^\alpha$; S es pues permutable con cada elemento del grupo cíclico $\langle x \rangle$. Tenemos entonces, por el segundo teorema de isomorfismo

$$S \cdot \langle x \rangle / S \simeq \langle x \rangle / S \cap \langle x \rangle.$$

El orden del grupo cociente $\langle x \rangle / S \cap \langle x \rangle$ divide al orden p^v de $\langle x \rangle$: es pues de la forma p^λ ; además $\lambda = 0$ implica $S \cap \langle x \rangle = \langle x \rangle$ es decir $\langle x \rangle \subseteq S$ ó $x \in S$, y recíprocamente.

Pero también tenemos

$$p^\lambda = O(S \cdot \langle x \rangle / S) = \frac{O(S \cdot \langle x \rangle)}{O(S)}$$

de donde

$$O(S \cdot \langle x \rangle) = p^{r+\lambda}.$$

Ahora, el orden de $S \cdot \langle x \rangle$, subgrupo de G divide al orden mp^r de G : esto exige $\lambda = 0$, de donde $x \in S$.

2.º Consideremos ahora, en un grupo G cualquiera, de una parte un subgrupo A y un subgrupo distinguido de A , A' ; por otra parte un subgrupo B y un subgrupo distinguido de B , B' . Pongamos

$$G' = A \cap B, \quad G'' = (A' \cap B) (A \cap B').$$

Por el lema 1, $A' \cap B$ y $A \cap B'$ son subgrupos distinguidos de $A \cap B = G'$ su producto G'' es por ello subgrupo distinguido de G' (cap. III, § 1).

A' , distinguido en A , es permutable con todo elemento de G' , en particular con todo elemento de G'' ; $A'G''$ y $A'G'$ son pues subgrupos de G y tenemos:

$$A'G'' \subseteq A'G' \quad A'G'' \cdot G' = A' \cdot G''G' = A'G'.$$

Esta última igualdad, según el lema 3, implica que $A'G''$ es subgrupo distinguido de $A'G'$, puesto que G'' , distinguido en G' , y A' son permutables con todo elemento de G' lo que implica que $A'G''$ lo es igualmente. Según el segundo

teorema de isomorfismo, $A'G'' \cap G'$ es subgrupo distinguido de G' y tenemos

$$(1) \quad A'G'/A'G'' = A'G'' \cdot G'/A'G'' \simeq G'/A'G'' \cap G'.$$

Ahora, puesto que G'' es subgrupo de G' tenemos $G'G'' = G'$, de donde

$$A'G'' \cap G' = A'G'' \cap G'G'' \supseteq (A' \cap G')G'',$$

pero todo elemento x de $A'G'' \cap G'$ es de la forma

$$x = g' = a'g'' \quad \text{donde} \quad a' \in A', g' \in G', g'' \in G'' \subseteq G'$$

lo que implica $a' \in G'$, luego $x \in (A' \cap G')G''$ y tenemos la igualdad

$$A'G'' \cap G' = (A' \cap G')G''.$$

Ahora bien,

$$A' \cap G' = A' \cap A \cap B = A' \cap B$$

y, puesto que $G'' = (A' \cap B)(A \cap B')$ contiene a $A' \cap B = A' \cap G'$,

$$(A' \cap G')G'' = G''.$$

Finalmente, (1) se escribe

$$(2) \quad A'G'/A'G'' \simeq G'/G''.$$

Puesto que G' y G'' son simétricos con respecto a los pares A, A' y B, B' , tenemos igualmente

$$B'G'/B'G'' \simeq G'/G'',$$

de donde, por la transitividad del isomorfismo,

$$A'G'/A'G'' \simeq B'G'/B'G''.$$

Reemplazando finalmente $A'G'$ y $A'G''$ por sus expresiones

$$\begin{aligned} A'G' &= A'(A \cap B), & A'G'' &= A'(A' \cap B)(A \cap B') \\ & & &= A'(A \cap B'), \end{aligned}$$

obtenemos el

Teorema de Zassenhaus. — Si A', B' son subgrupos distinguidos de A y B respectivamente, $A'(A \cap B')$ es subgrupo distinguido de $A'(A \cap B)$, $B'(A' \cap B)$ es subgrupo distinguido de $B'(A \cap B)$, y se tiene el isomorfismo

$$A \cap B / (A \cap B')(A' \cap B) \simeq A'(A \cap B) / A'(A \cap B') \simeq B'(A \cap B) / B'(A' \cap B).$$

Observación. — Hemos establecido el segundo teorema de isomorfismo y el teorema de Zassenhaus para un grupo ordinario G . Si G es un Δ -grupo esas propiedades permanecen válidas con los siguientes complementos.

Si en el segundo teorema de isomorfismo los subgrupos permutables G_1 y G_2 son Δ -subgrupos, lo mismo ocurre con su producto (y unión completa) $G_1 G_2$, con su intersección $G_1 \cap G_2$ y con los grupos cocientes $G_1 G_2 / G_1$ y $G_2 / G_1 \cap G_2$.

Como dos clases pertenecientes respectivamente a estos grupos cocientes se corresponden si tienen en común un elemento de G_2 , el isomorfismo es un Δ -isomorfismo.

Se ve igualmente que el teorema de Zassenhaus vale para los Δ -subgrupos. Los grupos cociente del enunciado son entonces Δ -subgrupos y el isomorfismo entre ellos es un Δ -isomorfismo.

§ 3. Series normales. Series de composición.

Teorema de Jordan-Hölder

En el retículo de los subgrupos de G se llama *serie normal* a todo subconjunto finito totalmente ordenado, o *cadena*, que va de G a E :

$$G_0 = G \supset G_1 \supset G_2 \supset \dots \supset G_k = \{e\} = E$$

con esta condición suplementaria: *todo G_i es subgrupo distinguido de G_{i-1} ($G_{i-1} \triangleright G_i$), aunque en general no lo es, naturalmente de G .*

Todo grupo admite series normales, por ejemplo $\{G, E\}$. Si H es subgrupo distinguido de G ($H \neq G, H \neq E$), $G \supset H \supset E$ es una sucesión normal que contiene a este subgrupo distinguido de G .

Los grupos cocientes $G/G_1, \dots, G_i/G_{i+1}, \dots, G_{k-1}/G_k = G_{k-1}, G_k = \{e\}$ se llaman *factores de la serie normal*, el número k de factores se llama *longitud* de la serie (número de sus elementos menos uno). Una serie normal

$$G \supset H_1 \supset \dots \supset H_l = E$$

se llama *subdivisión* de la primera si la primera es un subconjunto de ella (por lo tanto, si todos las G_i son H_j), en este caso $k \leq l$.

Dos series normales se llaman *isomorfas* si tienen la misma longitud y si sus grupos factores pueden asociarse biyectivamente de modo que los factores correspondientes sean grupos isomorfos

Teorema de Schreier. — *Dos series normales cualesquiera de un grupo G , admiten subdivisiones isomorfas.*

La demostración se basa en el teorema de Zassenhaus.

Sean

$$\begin{aligned} G &= G_0 \supset G_1 \supset G_2 \supset \dots \supset G_k = E \\ G &= H_0 \supset H_1 \supset H_2 \supset \dots \supset H_l = E \end{aligned}$$

dos series normales del grupo G .

Pongamos

$$G_{ij} = G_i (G_{i-1} \cap H_j) = G_i \vee (G_{i-1} \wedge H_j)$$

en el retículo de los subgrupos, e igualmente

$$H_{ij} = H_j (H_{j-1} \cap G_i).$$

como G_i y $G_{i-1} \cap H_j$ son dos subgrupos de G_{i-1} y puesto que G_i es distinguida en G_{i-1} , G_{ij} es subgrupo de G_{i-1} ; G_{ij} es además subgrupo distinguido de $G_{i,j-1}$ según el teorema Zassenhaus en que tomamos

$$\begin{aligned} A &= G_{i-1}, & B &= H_{j-1}, \\ A' &= G_i, & B' &= H_j. \end{aligned}$$

Podemos entonces formar las series parciales

$$\begin{aligned} G_{i-1} &= G_{i,0} \supseteq G_{i,1} \supseteq \dots \supseteq G_{i,l} = G_i \\ H_{j-1} &= H_{0,j} \supseteq H_{1,j} \supseteq \dots \supseteq H_{k,j} = H_j, \end{aligned}$$

Además, tenemos el isomorfismo

$$G_{i,j-1}/G_{ij} \simeq H_{i-1,j}/H_{ij},$$

porque el mismo, en efecto, puede escribirse:

$$G_i (G_{i-1} \cap H_{j-1})/G_i (G_{i-1} \cap H_j) \simeq H_j (H_{j-1} \cap G_{i-1})/H_j (H_{j-1} \cap G_i)$$

y este isomorfismo resulta del teorema de Zassenhaus.

Por lo tanto, si introducimos entre G_{i-1} y G_i los $l-1$ subgrupos G_{ij} , y así sucesivamente, y lo mismo hacemos en la serie de las H_j , obtendremos dos series de kl grupos, que pueden no ser cadenas, ya que dos grupos consecutivos pueden ser iguales, lo que da un grupo factor igual a E ; como los factores que se corresponden son isomorfos hay un mismo número de coincidencias en las dos sucesiones y las dos series normales isomorfas requeridas se obtienen suprimiendo todo subgrupo igual a su precedente.

Definición. — Se llama *serie de composición* de un grupo G (o serie de *Jordan-Hölder*) una serie normal finita *maximal* de G a E . Una serie tal

$$G = G_0 \supset G_1 \supset \dots \supset G_{i-1} \supset G_i \supset \dots \supset G_l = E$$

($G_i \triangleleft G_{i-1}$), si existe, es pues una serie normal que no admite subdivisión. Para que sea así es necesario y suficiente que G_i sea subgrupo distinguido maximal de G_{i-1} ($i = 1, \dots, l$) o, lo que es lo mismo, aplicando el primer teorema de isomorfismo al homomorfismo $G_{i-1} \sim G_{i-1}/G_i$, que el grupo cociente G_{i-1}/G_i sea *simple* (es decir no tenga ningún subgrupo distinguido propio).

La aplicación a las series de composición (eventuales) del teorema de Schreier da inmediatamente:

Teorema de Jordan-Hölder. — Si un grupo G admite diversas series de composición, dos cualesquiera de ellas son isomorfas.

Todo grupo finito tiene evidentemente series de composición. Se ve fácilmente que, por el contrario, un grupo monógeno infinito no las tiene.

Sea G un grupo que admite una *serie de composición*

$$(\Sigma) \quad G = G_0 \supset G_1 \supset \dots \supset G_l = E$$

Si una serie normal

$$(\Sigma') \quad G = H_0 \supset H_1 \supset \dots \supset H_r = E$$

no es una serie de composición, admite, según el teorema de Schreier, una subdivisión (Σ'_1) isomorfa a (Σ) ; esta subdivisión (Σ'_1) es pues una serie de composición. Así, en un grupo que admite una serie de composición, para toda serie normal que no sea de composición existe una subdivisión que sí lo es.

Se ve en particular, que por todo subgrupo distinguido S , pasa una serie de composición (subdivisión de la serie normal $G \supset S \supset E$).

Sea ahora G un grupo con un dominio de operadores Δ . Los resultados

precedentes se extienden inmediatamente a condición de imponer a una serie

$$G = G_0 \supset G_1 \supset \dots \supset G_{i-1} \supset G_i \supset \dots \supset E,$$

para que sea normal, que G_i sea *subgrupo distinguido permitido* de G_{i-1} . Se tendrá una serie de composición si G_i es subgrupo distinguido permitido maximal de G_{i-1} , es decir, si el grupo cociente G_{i-1}/G_i es simple en el sentido de los Δ -grupos, es decir, no tienen ningún Δ -subgrupo distinguido propio.

Con estas definiciones la teoría se aplica inmediatamente, puesto que se basa en los teoremas de isomorfismo que hemos extendido a los Δ -grupos. Además, el isomorfismo de los factores, convenientemente asociados, en dos series isomorfas, es aquí un Δ -isomorfismo.

§ 4. Producto directo de grupos

Definición 1. — G es *producto directo* de sus subgrupos A y B si y sólo si:

$$I \left\{ \begin{array}{l} 1) A \text{ y } B \text{ son subgrupos distinguidos de } G, \\ 2) G = AB, \\ 3) A \cap B = E = \{e\}; \end{array} \right.$$

y en este caso se escribe $G = A \times B$.

Si G es abeliano (y con notación aditiva), G es *suma directa* de sus subgrupos A y B si y sólo si:

$$\left\{ \begin{array}{l} 1) A \text{ y } B \text{ son subgrupos de } G, \\ 2) G = A + B, \\ 3) A \cap B = \{0\} \end{array} \right.$$

y se escribe $G = A \oplus B$.

Volviendo al caso no abeliano, la condición 2) expresa que todo elemento g de G se puede escribir $g = ab$, $a \in A$, $b \in B$. Esta representación es única, porque si se tuviese $ab = a'b'$, resultaría $a'^{-1}a = b'b^{-1}$ y en virtud de 3) este elemento sería e ; luego $a' = a$, $b' = b$.

Finalmente, si G es producto directo de A y B , todo elemento a de A es permutable con todo elemento b de B . En efecto $aba^{-1} \in B$ puesto que B es distinguido; $ba^{-1}b^{-1} \in A$ puesto que A es distinguido, luego $(aba^{-1})b^{-1} \in B$, $a(ba^{-1}b^{-1}) \in A$ y $aba^{-1}b^{-1} \in A \cap B$, luego $aba^{-1}b^{-1} = e$, $ab = ba$.

Estas propiedades pueden tomarse como una nueva definición de producto directo:

Definición 2. — Se dice que G es producto directo de sus subgrupos A y B si y sólo si:

- $$\left\{ \begin{array}{l} 1^*) \text{ todo elemento } g \text{ de } G \text{ puede escribirse} \\ \qquad \qquad \qquad g = ab \quad a \in A, \quad b \in B \\ 2^*) \text{ para cada } g \text{ dado, } a \text{ y } b \text{ están determinados de manera única;} \\ 3^*) \text{ todo elemento de } A \text{ es permutable con todo elemento de } B. \end{array} \right.$$

Veamos que esta definición implica efectivamente las propiedades que intervienen en la definición 1.

Según 1*) todo conjugado $A' = gAg^{-1}$ de A es de la forma $abAb^{-1}a^{-1}$ y se tiene, según 3*),

$$abAb^{-1}a^{-1} = baAa^{-1}b^{-1}$$

ahora bien, puesto que $a \in A$, tenemos $aAa^{-1} = A$, luego

$$A' = bAb^{-1} = Abb^{-1} = A;$$

A es subgrupo distinguido de G y lo mismo B . La propiedad 2) ha resultado de la 1*). En fin, sea $c \in A \cap B$; c admite las dos representaciones

$$c = ce \quad (c \in A, e \in B) \quad \text{y} \quad c = ec \quad (e \in A, c \in B)$$

lo que, según 2*) implica $c = e$: la propiedad 3) también se cumple.

A la descomposición en producto directo $G = A \times B$ está asociada, en virtud de 1*) y 2*) una partición de G en clases aB es $G/B \simeq A$ y lo mismo $B \simeq G/A$. Esto resulta también, al ser B distinguido, por el segundo teorema de isomorfismo

$$AB/A \simeq B/(A \cap B) = B$$

ya que $A \cap B = E$.

Problema. — Dados dos grupos A y B ¿puede construirse un grupo G que sea producto directo de dos subgrupos A^* y B^* isomorfos a A y B respectivamente?

Consideremos el grupo G producto de A y B es decir, como se ha visto, el conjunto de pares (a, b) con $a \in A$, $b \in B$, al que se da la ley de composición interna $(a, b)(a', b') = (aa', bb')$, donde aa' es el producto en A y bb' el producto en B . Si e_A, e_B indican los elementos neutros de A y B , el grupo G

admite $A^* = \{(a, e_B)\}$ como subgrupo isomorfo a A , y $B^* = \{(e_A, b)\}$ como subgrupo isomorfo a B ; la intersección de A^* y B^* se reduce al elemento neutro de G , (e_A, e_B) .

Todo elemento de A^* es permutable con todo elemento de B^* , y tenemos $G = A^*B^*$ ya que todo elemento (a, b) de G se escribe

$$(a, e_B)(e_A, b) \in A^*B^*.$$

En consecuencia, G es producto directo de sus subgrupos A^* y B^* .

Generalización. — Diremos que G es el producto directo de sus subgrupos G_i ($i = 1, \dots, n$) y escribiremos $G = G_1 \times G_2 \times \dots \times G_n$ si:

1º Todo G_i es subgrupo distinguido de G .

2º $G_1G_2 \dots G_n = G$.

3º $(G_1G_2 \dots G_{i-1}) \cap G_i = \{e\}$ ($i = 2, \dots, n$).

Consecuencias de esta definición. — Si se pone $H_{i-1} = G_1G_2 \dots G_{i-1}$, H_{i-1} es subgrupo distinguido de G .

Tomando en particular $i = n$, vemos que

1) H_{n-1} y G_n son subgrupos distinguidos de G .

2) $H_{n-1}G_n = G$.

3) $H_{n-1} \cap G_n = \{e\}$.

luego G es producto directo de H_{n-1} y G_n , todo elemento g de G se escribe de un modo único en la forma

$$g = hg_n \quad h \in H_{n-1} \quad g_n \in G_n$$

y todo $h \in H_{n-1}$ es permutable con todo $g_n \in G_n$; Resulta, en particular que todo $g_n \in G_n$ es permutable con todo elemento de G_i , ($i = 1, \dots, n-1$). Por recurrencia se obtiene que todo elemento g de G es representable de una manera, y sólo de una, como producto

$$g = g_1g_2 \dots g_n, \quad \text{donde } g_i \in G_i$$

y donde todo elemento de G_i es permutable con todo elemento de G_j ($i \neq j$). Recíprocamente, estas propiedades implican 1), 2) y 3).

La representación de G como producto directo no es en general única: en

particular, varios factores directos $G_1, G_2, \dots, G_k$ por ejemplo pueden reemplazarse por su producto

$$H = G_1 G_2 \dots G_k = G_1 \times G_2 \times \dots \times G_k,$$

En efecto: todo elemento g de G admite una, y sólo una, representación de la forma $g = h g_{k+1} \dots g_n$ y todo elemento de H es permutable con todo elemento de uno de los grupos $G_{k+1}, \dots, G_n$; se tiene pues

$$G = H \times G_{k+1} \times \dots \times G_n.$$

Recíprocamente, si en la descomposición directa

$$G = G_1 \times G_2 \times \dots \times G_n,$$

un factor directo, G_1 por ejemplo, admite una descomposición directa

$$G_1 = S_1 \times S_2 \times \dots \times S_p,$$

G admite la descomposición directa

$$G = S_1 \times S_2 \times \dots \times S_p \times G_2 \times \dots \times G_n$$

ya que todo elemento de un grupo $S_i (\subseteq G_1)$ es permutable con todo elemento de un grupo $G_j (2 \leq j \leq n)$, todo elemento g de G admite sucesivamente las dos descomposiciones

$$g = g_1 g_2 \dots g_n = s_1 s_2 \dots s_p g_2 \dots g_n$$

y esta última descomposición, como se ve inmediatamente, es única.

De aquí resulta, puesto que el orden de los factores puede variar, que para todo índice i tenemos:

$$3') \quad G_1 \dots G_{i-1} G_{i+1} \dots G_n \cap G_i = \{e\}$$

Recíprocamente, a causa de la inclusión

$$G_1 \dots G_{i-1} \subseteq G_1 \dots G_{i-1} G_{i+1} \dots G_n$$

3') implica

$$G_1 \dots G_{i-1} \cap G_i = \{e\}.$$

La condición 3') puede reemplazar a la 3).

Es importante señalar también, que si un grupo G es producto directo

$$G = G_1 \times G_2 \times \dots \times G_n$$

y se da para cada índice i un subgrupo H_i de G_i , todo elemento de H_i ($\subseteq G_i$) es permutable con todo elemento de H_j ($\subseteq G_j$; $j \neq i$). El producto $H_1 \dots H_n$ es un subgrupo de G y el producto es directo, pues para cualquiera de sus elementos x no cabe más que una representación

$$x = h_1 \dots h_n \quad (h_i \in H_i \subseteq G_i).$$

Generalización a una familia infinita de subgrupos. — Se dirá que G es producto directo de sus subgrupos G_i si y sólo si: 1.º todo elemento g de G es de un modo, y sólo de uno, producto de un número *finito* de elementos tomados en las G_i ; 2.º todo elemento de G_{i_1} es permutable con todo elemento de G_{i_2} ($i_1 \neq i_2$). Entonces es fácil comprobar que cada G_i sólo tiene el elemento e en común con los grupos engendrados con los restantes G_i , y que cada uno de ellos es subgrupo distinguido en G .

Definición. — Un grupo que no puede ser descompuesto en producto directo de subgrupos (propios) se llama *indescomponible en producto directo*.

Ejemplos. — 1. Los *grupos simples* (es decir, los que no tienen subgrupos distinguidos propios) son indescomponibles en producto directo.

2. Un grupo monógeno infinito $G = (a)$ es indescomponible en producto directo, puesto que dos subgrupos G_1, G_2 de G son monógenos: sean a^{n_1} y a^{n_2} sus generadores; $a^{n_1 n_2} \in G_1 \cap G_2$, luego $G_1 \cap G_2 \neq \{e\}$.

3. Consideremos el grupo aditivo de los racionales G y dos subgrupos cualesquiera G_1, G_2 de G . Sean

$$a_1 = m_1/n_1 \in G_1, \quad a_2 = m_2/n_2 \in G_2$$

con m_1, m_2, n_1, n_2 enteros. El elemento

$$m_1 m_2 = m_2 n_1 \cdot a_1 = m_1 n_2 \cdot a_2$$

pertenece a la intersección $G_1 \cap G_2$, luego $G_1 \cap G_2 \neq \{0\}$, y G es indescomponible.

4. Sea $G = (a)$ un grupo cíclico de orden p^α (p primo). Todo subgrupo de G es cíclico y puede, como sabemos, ser engendrado por a^r con r/p^α ; los subgrupos propios de G son pues los engendrados por $a^p, a^{p^2}, \dots, a^{p^{\alpha-1}}$ y como resultan incluidos unos en otros, G es indescomponible.

Ejemplos de descomposición en producto directo. — 1) *El grupo aditivo de los complejos* es suma directa del grupo aditivo de los reales con el de los imaginarios puros.

2) *El grupo multiplicativo de los reales (sin el cero)* es producto directo del grupo multiplicativo de los reales positivos y del grupo cíclico de orden dos engendrado por (-1) :

$$\{-1, 1\}.$$

3) *El grupo multiplicativo de los racionales positivos* es el producto directo de los grupos monógenos engendrados por los números primos.

4) En un grupo abeliano G sean a un elemento de orden r y b un elemento de orden s , con r y s primos entre sí. Entonces el producto ab es de orden rs . El orden del subgrupo $(a) \cap (b)$, divisor de r y s , es 1, luego

$$(a) \cap (b) = (e),$$

y el producto $(a)(b)$ es directo. Entonces la igualdad $(ab)^\rho = a^\rho b^\rho = e$ sólo tiene lugar si $a^\rho = e$, y $b^\rho = e$, es decir, si ρ es múltiplo de r y de s , luego de rs . Como $(ab)^{rs} = e$, el orden de ab es precisamente rs . Como el grupo engendrado por ab está incluido en el producto directo $(a) \times (b)$ y tiene su mismo orden, rs , estos dos grupos son el mismo. Estas propiedades se pueden aplicar al cálculo del indicador de Euler (cap. III, § 3).

5) Consideremos un grupo abeliano con torsión, es decir, en el que todo elemento es de orden finito.

Sea p un número primo. Consideremos el conjunto de los elementos a de G cuyo orden es potencia de p , y supongamos este conjunto A no vacío. En notación aditiva, sean $p^i a_i = 0$, $p^{i'} a_{i'} = 0$, entonces $p^{i+i'}(a_i - a_{i'}) = 0$, luego $a_i \in A$ y $a_{i'} \in A$ implican $a_i - a_{i'} \in A$. Así A es un subgrupo, llamado *p*-primario (se llama *grupo p-primario* a un grupo tal, que sus elementos tienen por orden la potencia de un número primo p).

Sea B el conjunto de elementos b de G cuyo orden n no es múltiplo de p sino, por consiguiente, primo con p . Si b_1, b_2 son dos elementos de B de orden n_1 y n_2 , $n_i b_i = 0$ y en consecuencia $n_1 n_2 (b_1 - b_2) = 0$; luego el orden de $b_1 - b_2$ divisor de $n_1 n_2$, es primo con p , y $b_1 - b_2 \in B$; B es, pues, un subgrupo de G .

Tenemos evidentemente $A \cap B = \{0\}$. Mostremos que $A + B = G$, y en-

tonces G será suma directa de A y B .

Sea $g \in G$, y n el orden de g ; pongamos $n = p^\alpha q$ con $(p, q) = 1$, luego $(p^\alpha, q) = 1$. Si $q = 1$, $g \in A$; si $\alpha = 0$, $g \in B$.

Sean, pues, $q \neq 1$, $\alpha \neq 0$. Existen dos enteros, u, v , que satisfacen la relación de Bezout $1 = up^\alpha + vq$; luego

$$g = (up^\alpha + vq)g = u(p^\alpha g) + v(qg);$$

pero $p^\alpha g$ es de orden q primo con p , luego $p^\alpha g \in B$, $b = u(p^\alpha g) \in B$, qg es de orden p^α , luego $qg \in A$ y $a = vqg \in A$; finalmente, $g = a + b$, c.q.d.

Entre los números primos p para los cuales no es vacío el conjunto A_p de elementos de G cuyo orden es potencia de p , tomemos ahora los n más pequeños, $p_1, \dots, p_n$, tendremos

$$G = A_1 \oplus A_2 \oplus \dots \oplus A_n \oplus B$$

donde ponemos $A_i = A_{p_i}$, y B es un subgrupo de G cuyos elementos son de orden no divisible por ningún primo $\leq p_n$.

En particular, si G es un grupo abeliano finito, es suma directa de un número finito de subgrupos p -primarios.

6) Sea G un grupo cíclico aditivo (a) de orden

$$N = p_1^{\alpha_1} \dots p_k^{\alpha_k} = p_1^{\alpha_1} n, \quad (p_1, n) = 1.$$

El elemento $a' = na$ es un elemento de orden $p_1^{\alpha_1}$, mientras que $a'' = p_1^{\alpha_1} a$ es de orden n . Se tiene pues $(a') \cap (a'') = 0$, $(a') + (a'') = G$, según el razonamiento anterior, luego G es la suma directa de esos dos subgrupos.

Descomponiendo (a') , se ve que: todo grupo cíclico $G = (a)$ de orden $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ es suma directa de subgrupos cíclicos p -primarios de órdenes

$$p_1^{\alpha_1}, \dots, p_i^{\alpha_i}, \dots, p_k^{\alpha_k},$$

engendrados respectivamente por

$$p_2^{\alpha_2} \dots p_k^{\alpha_k} a, \dots, p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_k^{\alpha_k} a, \dots, p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}} a.$$

Sea P un subgrupo de G del que se tiene la representación en producto directo

$$G = A_1 \times A_2 \times \dots \times A_n.$$

Consideremos los grupos $P_i = A_i \cap P$; P_i es subgrupo distinguido de P , por el lema 1 de § 2 (en el que se toma $H = G$, $S = A_i$, $K = P$).

Se tiene:

$$P_1 \dots P_{i-1} \subseteq A_1 \dots A_{i-1};$$

de donde

$$P_i \cap P_1 \dots P_{i-1} \subseteq A_i \cap A_1 \dots A_{i-1} = (e)$$

Los P_i factorizan pues un producto directo que es subgrupo de P :

$$P_1 \times P_2 \times \dots \times P_n \subseteq P.$$

En general no vale la igualdad, como muestra el ejemplo siguiente: Sea G el grupo aditivo de los vectores libres del plano xoy , y tomemos como grupos A_1, A_2 los subgrupos de vectores paralelos, respectivamente, a los ejes ox, oy , y como subgrupo P el de los vectores paralelos a una recta D distinta de los ejes. Tenemos

$$P_1 = A_1 \cap P = (0), \quad P_2 = A_2 \cap P = (0) \quad P_1 \oplus P_2 = (0) \subset P.$$

Si consideramos, por otra parte, para un elemento cualquiera de G , la representación

$$g = a_1 a_2 \dots a_i \dots a_n, \quad a_i \in A_i,$$

diremos que a_i es la *proyección* de g en A_i , o su *componente* en A_i . Designemos por A'_i el conjunto de proyecciones en A_i de los diversos elementos p de P ; entonces A'_i se llama *proyección de P en A_i* .

Todo elemento de $P_i = A_i \cap P$ tiene por proyección en A_j ($j \neq i$) el elemento neutro e , y es su propia proyección sobre A_i .

Resulta pues, para la proyección

$$P_i \subseteq A'_i \subseteq A_i$$

Pero además, A'_i es un subgrupo de G ; en efecto, si a'_i, a'_i son las proyecciones en A_i de dos elementos p, p' de P , $p = a_1 \dots a_i \dots a_n$, $p' = a'_1 \dots a'_i \dots a'_n$, $p^{-1}p'$ pertenece a P y como los elementos de A_λ son permutables con los de A_μ ($\lambda \neq \mu$) su proyección en A_i es $a_i^{-1}a'_i$ luego $a_i^{-1}a'_i \in A'_i$. Siendo cada elemento de A'_λ ($\subseteq A_\lambda$) permutable con cada elemento de A'_μ ($\subseteq A_\mu$), el producto $A'_1 \dots A'_n$ es un subgrupo de G y es el producto directo de los A'_λ , según una observación anterior.

Finalmente, hemos obtenido la doble inclusión

$$P_1 \times P_2 \times \dots \times P_n \subseteq P \subseteq A'_1 \times A'_2 \times \dots \times A'_n.$$

Observación. — En el ejemplo dado antes se tiene $A'_1 = A_1, A'_2 = A_2$, luego $P \subset A'_1 \oplus A'_2 = G$, con la inclusión estricta.

Si es $P_i = A'_i$ para $i = 1, 2, \dots, n$, resulta la doble igualdad

$$P_1 \times P_2 \times \dots \times P_n = P = A'_1 \times A'_2 \times \dots \times A'_n$$

Recíprocamente, cada una de esas dos igualdades implica

$$P_i = A'_i \quad (i = 1, \dots, n),$$

y, en consecuencia, cada una implica la otra.

Primeramente, si tenemos $P = P_1 \times \dots \times P_n$, la proyección A'_i de P en A_i es P_i .

Ahora, si $P = A'_1 \times \dots \times A'_n$, A'_i es subgrupo de P , luego tenemos $A'_i \subseteq A_i \cap P = P_i$, de donde la igualdad.

Observación. — Las $n - 1$ primeras condiciones $A'_i = P_i$ ($i = 1, \dots, n - 1$) implican la última. Sea $a'_n \in A'_n$ y $p = a'_1 \dots a'_{n-1}a'_n$ un elemento de P que tiene a'_n como componente en A_n . Tenemos

$$q = a'_1 \dots a'_{n-1} \in A'_1 \times \dots \times A'_{n-1} = P_1 \times \dots \times P_{n-1} \subset P$$

de donde $a'_n = q^{-1}p \in P$ y, por consiguiente, $a'_n \in P \cap A_n = P_n$; resulta $A'_n \subseteq P_n$, y de aquí la igualdad.

Ejemplos. — Sea $G = A_1 \times A_2 \times \dots \times A_n$ (producto directo). Designemos por Z el centro de G , por Z_i el de A_i y pongamos $P_i = Z \cap A_i$; llamemos A'_i a la proyección de Z en A_i : $P_i \subseteq A'_i$.

Sea $a'_i \in A'_i$; existe un elemento z de Z del que a'_i es la componente en A_i : $z = a'_1 \dots a'_i \dots a'_n$; z es permutable con un elemento cualquiera a_i de A_i , lo que exige $a_i a'_i = a'_i a_i$ de donde $a'_i \in Z_i$ y $A'_i \subseteq Z_i$.

Por otra parte, un elemento c_i de Z_i , permutable con todo elemento a_i de A_i y con todo elemento a_j de A_j ($j \neq i$), es permutable con todo elemento $x = a_1 \dots a_n$ de G ; luego $Z_i \subseteq Z$ lo que implica $Z_i \subseteq Z \cap A_i = P_i$.

Finalmente tenemos las inclusiones $P_i \subseteq A'_i \subseteq Z_i \subseteq P_i$, de donde la igualdad y, en consecuencia,

$$Z = Z_1 \times Z_2 \times \dots \times Z_n.$$

Enunciemos:

Teorema 1. — *El centro de un grupo G que es producto directo de sus subgrupos A_i es el producto directo de los centros de estos subgrupos.*

Teorema 2. — *Si un grupo G es un producto directo*

$$G = A_1 \times A_2 \times \dots \times A_n$$

su grupo conmutador C es el producto directo de los grupos conmutadores C_i de los A_i .

La proyección de un producto xy en A_i es el producto de las proyecciones, la proyección de un conmutador $xyx^{-1}y^{-1}$ es el conmutador $x_i y_i x_i^{-1} y_i^{-1}$ de las proyecciones. Tenemos pues, si A'_i designa la proyección de C en A_i , $A'_i \subseteq C_i \subseteq P_i = C \cap A_i$ y por consiguiente

$$A'_i = C_i = P_i;$$

el teorema queda establecido.

Señalemos para terminar las importantes ligaduras que hay entre las descomposiciones normales y las series directas o las series de composición.

Sea $G = A_1 \times A_2 \times \dots \times A_n$ un producto directo. Pongamos

$$G_i = A_{i+1} \times \dots \times A_n$$

(evidentemente producto directo) y formemos la serie

$$(\Sigma) \quad G = G_0 \supset G_1 \supset \dots \supset G_{i-1} \supset G_i \supset \dots \supset G_n = E$$

G_i es subgrupo distinguido de G ; *a fortiori* lo es de G_{i-1} ; Σ es pues una serie normal de G .

Además, tenemos

$$G_{i-1}/G_i = A_i \times G_i / G_i \simeq A_i;$$

luego, a la descomposición directa considerada corresponde una serie normal (Σ) cuyos factores son isomorfos a los componentes directos A_i .

En ciertos casos se puede pasar de esta serie normal (Σ) a una serie de composición. Así ocurre cuando cada A_i admite una serie de composición

$$(S_i) \quad A_i = B_{i,0} \supset B_{i,1} \supset \dots \supset B_{i,l_i} = (e)$$

Consideremos en efecto el homomorfismo canónico aplicando

$$G_{i-1} = A_i \times G_i$$

sobre A_i , con G_i como núcleo; según el primer teorema de isomorfismo a la serie (S_i) corresponde una parte de serie

$$(S'_i) \quad G_{i-1} = Q_{i,0} \supset Q_{i,1} \supset \dots \supset Q_{i,l_i} = G_i$$

en la cual $Q_{i,j}$ es subgrupo distinguido maximal de $Q_{i,j-1}$ puesto que B_{ij} es subgrupo distinguido maximal de $B_{i,j-1}$ y que tenemos el isomorfismo

$$Q_{i,j-1}/Q_{i,j} \simeq B_{i,j-1}/B_{i,j}.$$

Poniendo una tras otra las series S'_i , obtenemos para G una serie de composición S , que pasa por $G_1, G_2, \dots, G_{n-1}$ (o subdivisión de Σ) y de longitud

$$l = l_1 + l_2 + \dots + l_n.$$

Si, en particular, las A_i son grupos simples, las sucesiones S_i se reducen a

$$A_i \supset (e) \quad (l_i = 1)$$

y la serie de composición es la propia Σ : *todo producto directo de n grupos simples $A_1, A_2, \dots, A_n$ admite una serie de composición de longitud n cuyos factores son isomorfos a los A_i .*

Un grupo G que es producto directo de n grupos simples se llama *completamente reducible* o *semisimple*. Según el teorema de Jordan-Hölder, cuando un grupo G es semisimple, el número n de las componentes directas simples de que es producto, longitud de una serie de composición de G , está determinado de modo único; las componentes directas simples quedan determinadas salvo el orden y salvo isomorfismos.

Teorema 3. — *Dado un grupo semisimple*

$$G = A_1 \times A_2 \times \dots \times A_n$$

(donde las A_i son simples) y un subgrupo distinguido S de G , S es componente directa en una descomposición de G en la que los otros factores son ciertos A_i convenientemente elegidos.

El grupo G admite una serie de composición de longitud n ; se puede pues encontrar una serie de composición que pase por S (§ 3); la parte de esta serie

que va de S a $E = (e)$ es una serie de composición de S , de longitud l :

$$S = S_0 \supset S_1 \supset \dots \supset S_l = E.$$

Podemos escribir (con productos ordinarios)

$$G = SG = SA_1 \dots A_n.$$

Pongamos

$$\begin{aligned} H_1 &= S \\ H_2 &= SA_1 = H_1 A_1 \\ &\dots\dots\dots \\ H_{k+1} &= H_k A_k \\ &\dots\dots\dots \end{aligned}$$

Cada uno de los grupos H_k es distinguido en G . La intersección $H_k \cap A_k$, subgrupo distinguido de A_k que es simple, es igual a A_k o a E .

En el primer caso se tiene

$$A_k = H_k \cap A_k \subseteq H_k$$

Y por consiguiente $H_{k+1} = H_k A_k = H_k$: convendremos en suprimir A_k en el producto $SA_1 \dots A_n = G$.

En el segundo caso, $H_k \cap A_k = E$, el producto $H_{k+1} = H_k A_k$ es *directo*: $H_{k+1} = H_k \times A_k$; entonces conservaremos A_k .

Operando así sucesivamente obtenemos G en forma de producto directo, con S como primer factor:

$$G = S \times A_{i_1} \times \dots \times A_{i_r}.$$

A esta descomposición directa está asociada la serie de composición

$$G = S \times A_{i_1} \times \dots \times A_{i_r} \supset S \times A_{i_1} \times \dots \times A_{i_{r-1}} \supset \dots \supset S \supset S_1 \supset \dots \supset S_l = E$$

de longitud $r + l = n$; tenemos, pues, $r = n - l$.

Corolario. — *Todo subgrupo distinguido S de un grupo semisimple G es asimismo semisimple.*

Tenemos en efecto designando por $A_{j_1}, \dots, A_{j_l}$ los factores directos A_λ distintos de $A_{i_1}, \dots, A_{i_r}$:

$$S \simeq G/A_{i_1} \times \dots \times A_{i_r} \simeq A_{j_1} \times \dots \times A_{j_l}$$

el último grupo es semisimple, y es claro que un grupo isomorfo a uno semisimple también lo es.

Todo lo que precede se extiende inmediatamente al caso de los Δ -grupos. Cuando se trata de un grupo G con un dominio de operadores Δ , interesan generalmente las descomposiciones de G en producto directo de Δ -subgrupos distinguidos. Un producto de Δ -subgrupos distinguidos es él mismo un Δ -subgrupo (distinguido), por lo que las propiedades que acabamos de ver se aplican.

En esta extensión de la teoría, se dará al término de grupo simple el mismo sentido que al final del párrafo precedente: grupo que no admite Δ -subgrupo distinguido propio. Un grupo semisimple será un producto directo de tales grupos simples: las propiedades de estos grupos que conciernen a las series de composición (formadas de Δ -subgrupos) permanecen válidas; en el cap. IX haremos la aplicación a los espacios vectoriales ¹.

§ 5. Rango de un grupo abeliano G

Definición 1. — Un conjunto $\{\varphi_1, \dots, \varphi_k\}$ de elementos de G es un sistema ligado o sistema de elementos linealmente dependientes si existen enteros (≥ 0) $\alpha_1, \dots, \alpha_k$ no todos nulos tales que

$$\alpha_1\varphi_1 + \dots + \alpha_k\varphi_k = 0.$$

Un sistema en el que no sucede así se llama libre o linealmente independiente, y en este caso la igualdad

$$\alpha_1\varphi_1 + \dots + \alpha_k\varphi_k = 0 \quad \text{implica} \quad \alpha_i = 0 \quad (i = 1, \dots, k).$$

Un elemento u de G depende linealmente de $\{\varphi_1, \dots, \varphi_k\}$ si existen enteros $\alpha \neq 0, \beta_1, \dots, \beta_k$ tales que $\alpha u = \beta_1\varphi_1 + \dots + \beta_k\varphi_k$. Se escribe también en este caso $\alpha u \in (\varphi_1, \dots, \varphi_k)$.

Si a es de orden finito $r, ra = 0$, por lo que $\{a\}$ es un sistema linealmente dependiente, así como cualquier sistema que le contenga. Es inmediato que todo subconjunto de un sistema linealmente independiente es el mismo linealmente independiente. Más generalmente, un subconjunto infinito se dice linealmente independiente cuando no contiene a ningún conjunto finito linealmente dependiente.

Definición 2. — Dos subconjuntos finitos $\{u_1, \dots, u_k\}, \{\varphi_1, \dots, \varphi_l\}$, se dicen equivalentes y se escribe $\{u_1, \dots, u_k\} \sim \{\varphi_1, \dots, \varphi_l\}$, si todo u_i es lineal-

¹ El lector que lo crea conveniente puede pasar desde ahora al estudio de esas cuestiones, que no necesitan el conocimiento de los § 5, 6 de este capítulo.

mente dependiente de $\{v_1, \dots, v_l\}$ y si *recíprocamente* toda v_j es linealmente dependiente de $\{u_1, \dots, u_k\}$.

Esta propiedad es efectivamente transitiva porque

$$\alpha u_i \in (v_1, \dots, v_l), \alpha \neq 0, \text{ y } \beta_j v_j \in (w_1, \dots, w_k), \beta_j \neq 0$$

implican $\alpha\beta_1 \dots \beta_l u_i \in (w_1, \dots, w_k)$ y si $\{u_i\}$ y $\{v_j\}$ son dos sistemas equivalentes, todo elemento de G linealmente dependiente del primer sistema lo es del segundo y recíprocamente.

Teorema del cambio (de Steinitz). — Dado en G el sistema $\{u_1, \dots, u_k\}$ linealmente independiente, en el que todo u_i es linealmente dependiente de $\{v_1, \dots, v_l\}$ se tiene: $k \leq l$; y se pueden suprimir en el sistema $\{v_1, \dots, v_l\}$ k elementos, por ejemplo, $v_1, \dots, v_k$ y reemplazarlos por $u_1, \dots, u_k$ de tal modo que $\{u_1, \dots, u_k, v_{k+1}, \dots, v_l\}$ sea equivalente al sistema $\{v_1, \dots, v_l\}$.

Evidentemente basta con mostrar que los elementos $v_1, \dots, v_k$, son linealmente dependientes de $u_1, \dots, u_k, v_{k+1}, \dots, v_l$.

Demostración por recurrencia. — 1.º El teorema es cierto para $k = 1$: Supongamos u_1 linealmente independiente y dependiente del sistema $\{v_1, \dots, v_l\}$; $n_1 u_1 = \sum p_i v_i$, $n_1 \neq 0$. Entonces, existe al menos un $p_j \neq 0$, al que llamamos p_1 por ejemplo, y se tiene:

$$p_1 v_1 = -n_1 u_1 - \sum_{i \neq 1} p_i v_i.$$

2.º) Supongamos ahora el teorema cierto hasta $k-1$. Entonces,

$$\{u_1, \dots, u_{k-1}\} \subseteq \{u_1, \dots, u_{k-1}, u_k\}$$

es linealmente independiente, y sus elementos son linealmente dependientes de $v_1, \dots, v_l$, luego (con notaciones convenientes)

$$\{u_1, \dots, u_{k-1}; v_k, \dots, v_l\} \sim \{v_1, \dots, v_{k-1}; v_k, \dots, v_l\}$$

u_k , que es dependiente de $\{v_1, \dots, v_l\}$, es, pues, dependiente de

$$\{u_1, \dots, u_{k-1}, v_k, \dots, v_l\},$$

luego existen enteros $\alpha \neq 0$ y $\beta_1, \dots, \beta_l$ no todos nulos tales que

$$\alpha u_k = \beta_1 u_1 + \dots + \beta_{k-1} u_{k-1} + \beta_k v_k + \dots + \beta_l v_l$$

Se tiene $l \geq k$ pues las u_i son linealmente independientes, y por la misma razón, al menos un β_j ($k \leq j \leq l$) es $\neq 0$, sea $j = k$; tenemos:

$$(-\beta_k)v_k = \beta_1 u_1 + \dots + \beta_{k-1} u_{k-1} + (-\alpha)u_k + \beta_{k+1} v_{k+1} + \dots + \beta_l v_l,$$

luego

$$\{u_1, \dots, u_{k-1}, u_k, v_{k+1}, \dots, v_l\} \sim \{u_1, \dots, u_{k-1}, v_k, v_{k+1}, \dots, v_l\}$$

y se tiene en efecto

$$\{u_1, \dots, u_k, v_{k+1}, \dots, v_l\} \sim \{v_1, \dots, v_k, \dots, v_l\}.$$

Consecuencias. — 1) *Dos sistemas finitos linealmente independientes, equivalentes, de elementos de un grupo abeliano G , tienen el mismo número de elementos.* En efecto el resultado se aplica en los dos sentidos; se tiene

$$k \leq l \quad \text{y} \quad l \leq k \quad \text{de donde} \quad k = l.$$

De donde: *dos sistemas de generadores linealmente independientes tienen el mismo número de elementos.*

En un grupo con torsión, no tiene sistemas tales. Si el grupo no es un grupo con torsión, hay en él elementos linealmente independientes; los sistemas de elementos linealmente independientes, ordenados por inclusión, constituyen un subconjunto *inductivo* de G : Una cadena de sistemas S_i linealmente independientes admite un mayorante mínimo: $\bigcup S_i = S^*$. En efecto, S^* es un sistema linealmente independiente, pues si existen enteros $n_1, \dots, n_p$ y elementos $u_1, \dots, u_p$ de S^* tales que

$$n_1 u_1 + n_2 u_2 + \dots + n_p u_p = 0$$

cada u_i está contenido en una S_{v_i} ($i = 1, \dots, p$), y el mayor de los S_{v_i} contiene a $u_1, \dots, u_p$: como es linealmente independiente, tenemos

$$n_1 = \dots = n_p = 0.$$

De aquí, según el axioma de Zorn:

Si existen conjuntos linealmente independientes, cada uno está contenido en un conjunto linealmente independiente maximal.

Dos sistemas maximales son evidentemente equivalentes, luego:

En un grupo G dos sistemas linealmente independientes maximales supuestos finitos tienen el mismo número de elementos: este número se llama rango del grupo abeliano G .

Se puede decir que los grupos abelianos con torsión tienen el rango 0.

Como un sistema de generadores linealmente independientes es un sistema linealmente independiente maximal, *el número de estos generadores es el rango del grupo.*

Pero contrariamente a lo que sucede, como veremos, para los espacios vectoriales, un sistema linealmente independiente maximal no es en general un sistema de generadores del grupo. Tomemos por ejemplo como G el grupo monógeno infinito engendrado por a , $G = (a)$; todo elemento constituye un sistema linealmente independiente maximal, pero sólo los pares de elementos a y $-a$ son sendos sistemas de generadores.

Observaciones. — 1. Sea G un grupo de rango finito y A un subgrupo de G ; como todo sistema linealmente independiente en A lo es en G , todo sistema maximal en A está contenido en un sistema maximal de G , luego es de rango finito. Luego, *todo subgrupo A de un grupo G de rango finito es de rango finito.*

2. Consideremos el grupo cociente G/A : si se toma en un conjunto de clases linealmente independientes de G/A , $\{B_1, \dots, B_k\}$, representantes cualesquiera $b_1, \dots, b_k$, se obtiene un sistema de elementos de G linealmente independientes; pues si fuese

$$n_1 b_1 + n_2 b_2 + \dots + n_k b_k = 0$$

con algún n_i no nulo, se tendría $n_1 B_1 + n_2 B_2 + \dots + n_k B_k = 0$, y las B_i no serían linealmente independientes.

Luego, si el grupo G es de rango finito, todo sistema de elementos linealmente independientes maximal de G/A tiene un número finito de elementos, y G/A es de rango finito.

3. Sean $a_1, \dots, a_h$ elementos del subgrupo A de G que constituyen un sistema linealmente independiente maximal en A ; $B_1, \dots, B_k$ un sistema linealmente independiente maximal en G/A . Sea b_i un representante de B_i

$$B_i = b_i + A$$

Decimos que $\{a_1, \dots, a_h, b_1, \dots, b_k\}$ es un sistema linealmente independiente maximal de G .

Ante todo si se tuviese

$$\sum_{j=1}^h n_j a_j + \sum_{i=1}^k m_i b_i = 0$$

con los enteros n_j y m_i no todos nulos, se tendría en el grupo cociente G/A :

$$\sum_{i=1}^k m_i B_i = 0, \text{ lo que implica } m_i = 0 \ (i = 1, \dots, k).$$

Entonces queda $\sum_{j=1}^h n_j a_j = 0$ que, puesto que $\{a_j\}$ es un sistema linealmente independiente, implica $n_j = 0$, ($j=1, \dots, h$), y el sistema es linealmente independiente.

Si $a_1, \dots, a_h, b_1, \dots, b_k$, no fuese maximal, existiría $c \in G$, linealmente independiente de ese sistema. La clase $C = c + A$ de ese elemento sería linealmente independiente de $B_1, \dots, B_k$ (pues si no, c sería dependiente de $\{a_1, \dots, a_h, b_1, \dots, b_k\}$, pero es imposible que $\{B_1, \dots, B_k, C\}$ sea un sistema linealmente independiente de G/A , puesto que $B_1, \dots, B_k$ es maximal).

Se tiene pues:

$$\text{rango de } A + \text{rango de } G/A = \text{rango de } G.$$

4. Se ha visto que si G es la suma directa de dos subgrupos A y B

$$G = A \oplus B$$

B es isomorfo a G/A . Como dos grupos isomorfos tienen evidentemente el mismo rango, porque la independencia y carácter maximal de los sistemas independientes se conservan en el isomorfismo, se tiene

$$\text{rango de } G = \text{rango de } A + \text{rango de } B$$

y, reiterando:

Teorema 1. — Si un grupo abeliano G de rango finito es la suma directa de un número finito de sus subgrupos $S_1, \dots, S_p$, el rango de G es la suma de los rangos de los sumandos

Por otra parte, sea todavía

$$G = A \oplus B, \quad B \simeq G/A. \quad \text{PROPIEDADES}$$

Supongamos ahora A y B de rangos finitos y sean $\{a_1, \dots, a_k\}$ y $\{b_1, \dots, b_l\}$ sistemas maximales de A y de B respectivamente. Este $\{b_1, \dots, b_l\}$ es por consiguiente un representante de un sistema linealmente independiente $\{B_1, \dots, B_l\}$ de G/A . Se ha visto que $\{a_1, \dots, a_k, b_1, \dots, b_l\}$ es un sistema linealmente independiente maximal de G : luego G es de rango finito. Reiterando se obtiene:

Teorema 2. — *La suma directa de un número finito de grupos de rango finito es también de rango finito, y su rango es la suma de los rangos de los sumandos.*

5. Consideremos en particular en el grupo G el subgrupo T , conjunto de elementos de orden finito: T es el máximo subgrupo con torsión. Tenemos:

rango de $T = 0$, luego $\text{rango } G = \text{rango } I$ (con $I = G/T$), luego:

el rango de un grupo abeliano mixto es igual al rango del grupo factor con respecto a su subgrupo con torsión máximo.

§ 6. Grupos abelianos de tipo finito

Un grupo abeliano de tipo finito es isomorfo a un grupo cociente de un grupo abeliano libre con un número finito de generadores por uno de sus subgrupos (cap. III, § 7, teor. 1).

Señalemos primeramente que los generadores de un grupo abeliano libre constituyen un sistema de elementos linealmente independientes *maximal*. Luego:

Teorema 1. — *El número de generadores de un grupo abeliano libre de tipo finito G es el rango de G .*

Además, en virtud de las propiedades vistas precedentemente, *un grupo abeliano libre es la suma directa de los grupos monógenos engendrados por sus generadores.*

Se dice también que los generadores constituyen una *base* del grupo abeliano.

Vamos a establecer la siguiente propiedad fundamental:

Teorema 2. — *Todo subgrupo V de un grupo abeliano libre U_n de rango n es él mismo un grupo abeliano libre y su rango k es menor o igual a n . Además, se pueden escoger en U_n una base $x_1, \dots, x_n$, y en V una base $v_1, \dots, v_k$ tales que $v_i = \epsilon_i x_i$, $i = 1, 2, \dots, k$, siendo los $\epsilon_1, \dots, \epsilon_k$ enteros positivos tales que ϵ_i divida a ϵ_{i+1} para $i = 1, 2, \dots, k - 1$.*

Demostración por recurrencia.

Para $n = 1$, el enunciado se reduce a un teorema conocido: todo subgrupo V de un grupo monógeno $U_1 = (a)$, es monógeno y engendrado por na (a^n en notación multiplicativa).

Supongamos el teorema cierto para todo grupo de rango hasta $n - 1$.

Sea $V \subseteq U_n$, $V \neq \{0\}$ y $\{u_1, \dots, u_n\}$ una base de U_n . Todo elemento de V es de la forma $v = \sum n_i u_i$, con los n_i enteros.

Sea m el mínimo entero positivo que interviene como coeficiente en las expresiones $\sum n_i u_i$ pertenecientes a V (como al mismo tiempo que la dicha pertenece a V la $-\sum n_i u_i$, se pueden considerar sólo los n_i positivos).

Si se cambia de base para U_n el mínimo entero m asociado a la nueva base no es necesariamente el mismo.

Elijamos una base para la que este entero sea lo menor posible; le designaremos por ϵ_1 y por u_1 el elemento de la base del que es coeficiente en alguna de las expresiones en que interviene; sea ν_1 el elemento de V constituido por esa expresión:

$$\nu_1 = \epsilon_1 u_1 + \alpha_2 u_2 + \dots + \alpha_n u_n$$

Dividiendo α_i por ϵ_1 , con cociente $q_i \geq 0$,

$$\alpha_i = \epsilon_1 q_i + r_i, \quad 0 \leq r_i < \epsilon_1,$$

ν_1 se escribe

$$\nu_1 = \epsilon_1(u_1 + q_2 u_2 + \dots + q_n u_n) + r_2 u_2 + \dots + r_n u_n$$

Tomemos como nueva base:

$$\bar{u}_1 = u_1 + q_2 u_2 + \dots + q_n u_n, \quad \bar{u}_2 = u_2, \dots, \bar{u}_n = u_n.$$

Se tiene

$$\nu_1 = \epsilon_1 \bar{u}_1 + r_2 \bar{u}_2 + \dots + r_n \bar{u}_n.$$

Pero ϵ_1 es el menor entero positivo que interviene como coeficiente en un elemento de V cualquiera que sea la base elegida; se tiene pues

$$r_2 = \dots = r_n = 0,$$

de donde

$$\nu_1 = \epsilon_1 \bar{u}_1$$

Consideremos entonces el subgrupo V ; en él, $\nu_1 \in V$ engendra el subgrupo monógeno (ν_1) de V . Llamemos V' al subconjunto de elementos de V cuya representación en la base $\bar{u}_1, \dots, \bar{u}_n$, tiene 0 como coeficiente de $\bar{u}_1$:

$$V' = \left\{ \nu'; \nu' \in V, \nu' = \sum_{i=2}^n \beta_i \bar{u}_i \right\}.$$

$V' = V \cap (\bar{u}_2, \dots, \bar{u}_n)$ es un subgrupo y se tiene $(\nu_1) \cap V' = \{0\}$. Si $V' = \{0\}$,

$V = (\nu_1)$, y el teorema está demostrado. Mostremos que si $V' \neq 0$, V es la suma directa $(\nu_1) \oplus V'$.

Es suficiente demostrar que V es la suma ordinaria $(\nu_1) + V'$ y para ello que se tiene $V \subseteq (\nu_1) + V'$. Sea

$$\nu = \alpha_1 \bar{u}_1 + \alpha_2 \bar{u}_2 + \dots + \alpha_n \bar{u}_n \in V, \quad \text{donde } |\alpha_i| \geq \epsilon_1 \text{ (si } \alpha_i \neq 0 \text{)}.$$

Si $\alpha_1 = 0$, se tiene $\nu \in V' \subseteq (\nu_1) + V'$. Sea pues $\alpha_1 \neq 0$. Se tiene

$$\alpha_1 = \epsilon_1 q + r_1 \quad (0 \leq r_1 < \epsilon_1) \quad \text{y como} \quad \epsilon_1 q \bar{u}_1 \in (\nu_1) \subseteq V, \\ \nu - \epsilon_1 q \bar{u}_1 = r_1 \bar{u}_1 + \alpha_2 \bar{u}_2 + \dots + \alpha_n \bar{u}_n \in V.$$

Ahora bien, r_1 no puede ser un entero positivo $< \epsilon_1$; luego $r_1 = 0$, y

$$\alpha_2 \bar{u}_2 + \dots + \alpha_n \bar{u}_n = \nu' \in V'$$

de donde

$$\nu = \epsilon_1 q \bar{u}_1 + \nu'$$

lo que demuestra que en efecto $V \subseteq (\nu_1) + V'$ y, por consiguiente $V = (\nu_1) \oplus V'$.

Pero V' es un subgrupo del grupo libre de rango $n - 1$.

$$U_{n-1} = (\bar{u}_2, \dots, \bar{u}_n).$$

Por la hipótesis de recurrencia podremos elegir la base $\bar{\bar{u}}_2, \dots, \bar{\bar{u}}_n$, de U_{n-1} de modo que V' tenga por base $\nu_2, \dots, \nu_k$, con $\nu_i = \epsilon_i \bar{\bar{u}}_i$, $\epsilon_i > 0$ y ϵ_i divisor de ϵ_{i+1} .

Se tienen así para U la base $(\bar{u}_1, \bar{u}_2, \dots, \bar{u}_n)$ y para V la base $(\nu_1, \nu_2, \dots, \nu_k)$, con $\nu_1 = \epsilon_1 \bar{u}_1$, $\nu_2 = \epsilon_2 \bar{\bar{u}}_2$, ..., $\nu_k = \epsilon_k \bar{\bar{u}}_k$

$$\epsilon_i \text{ divisor de } \epsilon_{i+1} \quad (2 \leq i \leq k - 1).$$

Se tiene, pues, $k \leq n$, y queda por demostrar que ϵ_1 divide a ϵ_2 . Sea

$$\epsilon_2 = q_1 \epsilon_1 + r_2, \quad 0 \leq r_2 < \epsilon_1.$$

El elemento $\nu_2 = \epsilon_2 \bar{\bar{u}}_2$ de V se escribe $\nu_2 = q_1 \epsilon_1 \bar{\bar{u}}_2 + r_2 \bar{\bar{u}}_2$ y

$$\nu_2 - \nu_1 = \epsilon_1 (-\bar{u}_1 + q_1 \bar{\bar{u}}_2) + r_2 \bar{\bar{u}}_2.$$

En la base $\bar{\bar{u}}_1 = -\bar{u}_1 + q_1 \bar{\bar{u}}_2, \bar{\bar{u}}_2, \dots, \bar{\bar{u}}_n$, el elemento $\nu = \nu_2 - \nu_1$ de V

admite la representación $v = \epsilon_1 \bar{u}_1 + r_2 \bar{u}_2$, con $0 \leq r_2 < \epsilon_1$, lo que exige $r_2 = 0$, y tenemos $\epsilon_2 = q_1 \epsilon_1$.

Puesto que ϵ_1 divide a ϵ_2 la base de U formada por los elementos $x_1 = \bar{u}_1$, $x_2 = \bar{u}_2$, ..., $x_n = \bar{u}_n$ y la base $v_1, \dots, v_k$ de V tienen finalmente las condiciones enunciadas.

Teorema de estructura fundamental. — *Todo grupo abeliano de tipo finito G , escrito en forma aditiva, es suma directa de un número finito de grupos monógenos.*

Sea n el número de elementos de un sistema de generadores de G . Utilizaremos la propiedad de que G es isomorfo al grupo factor de un grupo abeliano libre U_n con relación a uno de sus subgrupos V , $G \simeq U_n/V$. Escojamos en U_n y V bases $(u_1, \dots, u_n)$ y $(v_1, \dots, v_k)$ tales que

$$v_i = \epsilon_i u_i, \quad \epsilon_i > 0, \quad \text{para } i = 1, 2, \dots, k, \quad (k \leq n)$$

con ϵ_i divisor de ϵ_{i+1} para $i = 1, 2, \dots, k-1$;

lo que es posible por el anterior teorema.

En estas condiciones $u = \alpha_1 u_1 + \dots + \alpha_n u_n \in U_n$ es un elemento de V si y sólo si:

$$\begin{cases} \alpha_i \text{ es divisible por } \epsilon_i \text{ para } i = 1, \dots, k \\ \alpha_j = 0 \text{ para } j = k+1, \dots, n. \end{cases}$$

La condición es evidentemente suficiente, pues si se cumple tenemos, poniendo

$$\alpha_i = q_i \epsilon_i \quad (i = 1, \dots, k), \quad u = q_1 v_1 + \dots + q_k v_k \in V$$

y recíprocamente, si $u \in V$, se tiene

$$u = \sum_{i=1}^k n_i v_i = \sum_{i=1}^k n_i \epsilon_i u_i$$

lo que implica la propiedad para las α_i porque la representación de un elemento u es única.

Puesto esto, es suficiente establecer el teorema para el grupo U_n/V isomorfo a G . Estudiemos el grupo factor $U_n/V = \{ \dots, u + V, \dots \}$. Consideremos las clases $\bar{u}_i = u_i + V$; se tiene, para $i \leq k$

$$\epsilon_i \bar{u}_i = \epsilon_i u_i + V = v_i + V = V = 0 \quad (\in U_n/V).$$

Si es $\epsilon_i = 1$ para $i = 1, 2, \dots, r-1$, se tiene $u_i \in V$ y $\bar{U}_i = 0$ para $i = 1, 2, \dots, r-1$ (y recíprocamente $\bar{U}_i = 0$ implica $\epsilon_i = 1$). Si $\epsilon_i > 1$ para $(1 \leq) r \leq i \leq k (\leq n)$, las clases correspondientes $\bar{U}_i$ de U_n/V son tales que $\epsilon_i \bar{U}_i = 0$; son, pues, de orden finito, divisor de ϵ_i y, en realidad igual a ϵ_i , puesto que $\lambda u_i \in V$ solamente si λ es múltiplo de ϵ_i . Finalmente, para $i > k$, se tiene $p_i u_i \notin V$, $\forall p_i \in \mathbb{Z}$, y las clases correspondientes $\bar{U}_i$ engendran grupos monógenos infinitos.

Puesto que todo $u \in U_n$ se escribe $u = \alpha_1 u_1 + \dots + \alpha_n u_n$, de un modo y sólo de uno, en U_n/V toda clase $\bar{U} = u + V$ se escribe

$$\bar{U} = \alpha_r \bar{U}_r + \dots + \alpha_k \bar{U}_k + \dots + \alpha_n \bar{U}_n$$

donde las $\bar{U}_i$ engendran grupos monógenos, finitos para $i = r, \dots, k$, infinitos para $i = k+1, \dots, n$.

El grupo U_n/V es pues la suma de estos grupos monógenos y es en efecto una suma *directa*, puesto que de haber una segunda representación

$$\bar{U} = \beta_r \bar{U}_r + \dots + \beta_n \bar{U}_n$$

resulta, al designar $u = \alpha_1 u_1 + \dots + \alpha_n u_n$ un representante de $\bar{U}$,

$$u = \beta_r u_r + \dots + \beta_n u_n + v, \quad \text{con} \quad v = n_1 \epsilon_1 u_1 + \dots + n_k \epsilon_k u_k,$$

de donde, puesto que la representación $u = \alpha_1 u_1 + \dots + \alpha_n u_n$ es única,

$$\alpha_i = \beta_i + n_i \epsilon_i \text{ para } i = 1, \dots, k \quad \text{con} \quad \beta_i = 0 \text{ para } i = 1, \dots, r-1;$$

$$\alpha_i = \beta_i \text{ para } i = k+1, \dots, n$$

lo que implica

$$\alpha_i \bar{U}_i = \beta_i \bar{U}_i \text{ para } i = r, \dots, k, \dots, n.$$

Finalmente, la propiedad queda demostrada para G , que es isomorfo a U_n/V .

Se ha visto que un grupo monógeno infinito es indescomponible; y que un grupo monógeno finito (esto es, cíclico) de orden $N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ es suma directa de grupos cíclicos indescomponibles de orden $p_i^{\alpha_i}$. Luego:

Todo grupo abeliano de tipo finito G es suma directa de un número finito de grupos monógenos indescomponibles: unos infinitos, otros finitos y primarios. Los generadores de cada uno de estos grupos monógenos constituyen lo que se llama una base de G .

Los generadores de grupos monógenos infinitos constituyen un sistema de

mentos linealmente independiente maximal; su número es, pues, lo que hemos llamado *rango* de G .

Se ha visto que el rango de G es un número asignado de una manera intrínseca a G . Luego, cualesquiera sean el grupo libre U_n que se considere asociado a G y a un sistema de generadores de G , y la base elegida en U_n satisfaciendo a las condiciones del teorema de subgrupo de un grupo libre, se encontrará para G una representación en suma directa de grupos monógenos indescomponibles *que contiene siempre el mismo número de grupos monógenos infinitos*.

Vamos a demostrar que *el conjunto de los órdenes de los sumandos cíclicos primarios es también independiente de la descomposición*.

Puesto que todo grupo abeliano G de tipo finito es la suma directa de un número finito de grupos monógenos de orden $p_i^{\alpha_i}$ y de un número finito de grupos monógenos infinitos, se tiene, considerando la suma directa de los primeros y la suma directa de los últimos, una descomposición intrínseca de todo grupo abeliano de tipo finito en suma directa de un subgrupo con torsión máximo T , y de una parte sin torsión L . Componiendo los grupos monógenos de orden $p_i^{\alpha_i}$ relativos a un mismo p_i , se tiene un grupo p_i -primario A_{p_i} , y de este modo se tiene la representación de T en suma directa de grupos p_i -primarios que tienen una significación intrínseca (§ 4, ejemplo 5). Por consiguiente, nos bastará demostrar la proposición sólo para un grupo p -primario finito.

Sea pues G un grupo p -primario finito y H un subgrupo de G . Mostremos primero que el número de subgrupos cíclicos p -primarios de H , s , en una descomposición cualquiera es inferior al número t de componentes de G en la representación considerada, y que, si para G los órdenes de estos componentes son:

$$p^{\alpha_1}, \dots, p^{\alpha_t}, \quad \alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_t,$$

y para H :

$$p^{\beta_1}, \dots, p^{\beta_s}, \quad \text{con} \quad \beta_1 \geq \beta_2 \geq \dots \geq \beta_s$$

entonces, se tiene

$$\alpha_i \geq \beta_i, \quad i = 1, 2, \dots, s, \quad s \leq t.$$

Tomando $H = G$ y aplicando esta propiedad para las dos descomposiciones así obtenidas de G , se tendrá, como enunciamos,

$$s \leq t \text{ y } t \leq s \text{ de donde } t = s$$

y

$$\alpha_i \leq \beta_i, \beta_i \leq \alpha_i; \text{ de donde } \alpha_i = \beta_i, i = 1, \dots, s.$$

Sea pues

$$\begin{aligned} G &= (a_{\alpha_1}) \oplus \dots \oplus (a_{\alpha_s}) & a_{\alpha_i} \text{ de orden } p^{\alpha_i} (\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_s) \\ H \subseteq G & \quad H = (b_{\beta_1}) \oplus \dots \oplus (b_{\beta_t}) & b_{\beta_i} \text{ de orden } p^{\beta_i} (\beta_1 \geq \beta_2 \geq \dots \geq \beta_t). \end{aligned}$$

Calculemos el número de elementos de G de orden p .

En (a_{α_i}) se tiene el elemento $p^{\alpha_i-1} a_{\alpha_i} = a_i$ que engendra un subgrupo cíclico de orden p , en que todos los elementos no nulos son de orden p , puesto que p es primo, y el subgrupo suma directa

$$(a_1) \oplus \dots \oplus (a_s),$$

está constituido del 0 y de elementos de orden p . Este subgrupo agota el conjunto de los elementos de orden p , puesto que un elemento $g = g_1 + g_2 + \dots + g_t$ de G con $g_i \in (a_{\alpha_i})$, tiene por orden el mínimo común múltiplo de los órdenes de $g_1, \dots, g_t$, y este orden no puede ser p a menos que cada elemento g_i sea nulo o de orden p . Ahora bien, (a_i) es el conjunto de los elementos de (a_{α_i}) de orden p .

El número de estos elementos es pues el orden de $(a_1) \oplus \dots \oplus (a_s)$ es decir, p^s , con un significado intrínseco, independiente de la descomposición, luego s es un invariante del grupo. En todo subgrupo H el número de elementos de orden p no puede pues superar a p^s ; como este número es p^t , se tiene efectivamente $t \leq s$.

Falta demostrar que $\beta_i \leq \alpha_i$, para $i = 1, 2, \dots, s$.

Supongamos lo contrario, esto es, que exista un entero j tal que

$$\begin{aligned} \beta_i &\leq \alpha_i \quad \text{para } i \leq j-1 & (j \geq 1) \\ \beta_j &> \alpha_j \end{aligned}$$

Consideremos el conjunto D de los elementos de G de la forma $p^{\alpha_j} x$, donde $x \in G$. Puesto que $p^{\alpha_j} x - p^{\alpha_j} x' = p^{\alpha_j} (x - x')$, con $x' \in G$, es un elemento de D , D es un subgrupo de G .

Todo elemento de D en la representación de G considerada es de la forma $p^{\alpha_j} c_1 + \dots + p^{\alpha_j} c_t$, con $c_i \in (a_{\alpha_i})$. La proyección de D en (a_{α_i}) es pues $(p^{\alpha_j} a_{\alpha_i})$ y este grupo cíclico es también $D \cap (a_{\alpha_i})$. Luego (§ 4):

$$D = (p^{\alpha_j} a_{\alpha_1}) \oplus (p^{\alpha_j} a_{\alpha_2}) \oplus \dots \oplus (p^{\alpha_j} a_{\alpha_s}).$$

Pero $p^{\alpha_i} a_{a_k} = 0$ para $k \geq j$. Luego:

$$D = (p^{\alpha_i} a_{a_1}) \oplus \dots \oplus (p^{\alpha_i} a_{a_{j-r}}), \quad \text{donde } a_{j-r} > a_j, a_{j-r+1} = a_j$$

y este subgrupo D de G es suma directa de a lo más $j - 1$ grupos cíclicos p -primarios.

Pero los elementos de H de la forma $p^{\alpha_i} x, x \in H$, forman un subgrupo K de H que es también la suma directa

$$K = (p^{\alpha_i} b_{\beta_1}) \oplus (p^{\alpha_i} b_{\beta_2}) \oplus \dots \oplus (p^{\alpha_i} b_{\beta_h})$$

donde h es el último índice para el cual $\beta_h > a_j$; se tiene por hipótesis $h \geq j$.

Luego, en la descomposición de K en suma directa de subgrupos cíclicos p -primarios hay *al menos* j componentes, mientras que habíamos encontrado a lo más $j - 1$ para D . Como K es subgrupo de D esto es imposible, según la primera parte de la demostración, y la proposición queda demostrada.

El rango del grupo abeliano de tipo finito y los enteros $\alpha_1, \dots, \alpha_s$ de los diferentes sumandos cíclicos p -primarios, constituyen el *sistema completo de invariantes* del grupo.

CAPITULO IX

ESPACIOS VECTORIALES

§ 1. Espacios vectoriales como grupos con operadores¹

Dado un cuerpo Δ , que aquí supondremos conmutativo, un *espacio vectorial* sobre Δ se ha definido (cap. VIII, § 1) como un grupo abeliano E , aditivo, admitiendo a Δ como dominio de operadores, lo que implica

$$(1) \quad a(x + y) = ax + ay \quad \forall x, y \in E \quad y \quad \forall a \in \Delta,$$

y cumpliendo las condiciones suplementarias

$$(2) \quad (a + \beta)x = ax + \beta x \quad \forall x \in E \quad y \quad \forall a, \beta \in \Delta,$$

$$(3) \quad a(\beta x) = (a\beta)x \quad \forall x \in E \quad y \quad \forall a, \beta \in \Delta,$$

$$(4) \quad \epsilon x = x \quad \forall x \in E$$

en donde ϵ designa el elemento-unidad de Δ . A los elementos de E se les llama *vectores*. Las condiciones precedentes implican

$$0x = \bar{0} \quad (0 \in \Delta, \bar{0} \in E) \quad y \quad ax \neq \bar{0} \quad \text{cuando} \quad a \neq 0 \quad (\in \Delta) \quad y \quad x \neq \bar{0} \quad (\in E).$$

Hemos visto también, que todo subgrupo lícito A de E es de hecho un espacio vectorial sobre Δ y, por esta razón, los Δ -subgrupos de E han sido llamados *subespacios* de E . Los subespacios de E forman una familia de Moore, y por ende un retículo completo, donde la intersección conjuntista es el ínfimo y la suma es el supremo; este retículo no es distributivo, pero sí es modular (cap. VIII, § 1).

A la familia de Moore $\mathcal{S}$ de los subespacios corresponde una clausura de Moore que asocia a todo subconjunto M de E el mínimo subespacio $\overline{M}$ que

¹ El estudio de los espacios vectoriales de base finita es independiente del axioma de Zorn, como se expone en la última parte de este § 1. y recomendamos empezar ahí (pág. 321) el estudio del capítulo, al lector que no esté especialmente interesado en lo anterior. (N. del T.)

contenga a M , al que se llama subespacio engendrado por M . En general, $\overline{M}$ no coincide con el subgrupo aditivo engendrado por M . En efecto, consideremos por ejemplo el espacio E de vectores reales del plano xOy , sobre el cuerpo real $\mathbf{R}$, y tomemos para M el conjunto $\{\vartheta\}$ constituido por el vector $(1, 0)$. El subgrupo engendrado por M es el conjunto de los vectores $(n, 0)$ donde $n \in \mathbf{Z}$, mientras que el subespacio $\overline{M}$ engendrado por M es el conjunto de vectores $(x, 0)$ donde $x \in \mathbf{R}$.

Si $\vartheta_1, \vartheta_2, \dots, \vartheta_k$ son k vectores de M , y si $\lambda_1, \lambda_2, \dots, \lambda_k$ son k elementos del cuerpo Δ , el subespacio $\overline{M}$ engendrado por M contiene el vector llamado *com-*

$$\lambda_1\vartheta_1 + \lambda_2\vartheta_2 + \dots + \lambda_k\vartheta_k$$

binación lineal de los vectores ϑ_i ; por definición, los λ_i son los *coeficientes* de esta combinación lineal.

Sea M^* el conjunto de las combinaciones lineales de un número cualquiera de vectores de M , con coeficientes cualesquiera. Según lo que precede tenemos

$$M^* \subseteq \overline{M}.$$

Es inmediato que M^* es un grupo aditivo y un subconjunto lícito. M^* es, pues, un subespacio; por construcción, contiene a M . Tenemos entonces $\overline{M} \subseteq M^*$, por tanto vale el signo de igualdad, y podemos enunciar.

Teorema 1. — *El conjunto M^* de las combinaciones lineales de vectores pertenecientes a un conjunto dado M es un espacio vectorial, que coincide con el subespacio $\overline{M}$ engendrado por M :*

$$M^* = \overline{M}.$$

Un espacio vectorial (o un subespacio vectorial) engendrado por un solo vector ϑ se llama *monógeno*.

Teorema 2. — *En un espacio vectorial E sobre el cuerpo Δ , son una misma cosa los subespacios monógenos y los Δ -subgrupos simples.*

El teorema es evidente para el subespacio (0) y el subgrupo (0) . Demostremoslo para subespacios y subgrupos diferentes de (0) .

1.º Sean $S = (\vartheta)$ un subespacio monógeno de E , distinto de (0) y S' un Δ -subgrupo no nulo de S :

$$(0) \subset S' \subseteq S = (\vartheta).$$

Por hipótesis, S' contiene un vector $\omega \neq 0$; tendremos $\omega = a\vartheta$ y $a \neq 0$; pero,

entonces, $\varphi = \alpha^{-1}\omega$ pertenece a S' , lo que implica $S' = S$: S es simple.

2.º Inversamente, sean S un Δ -subgrupo simple no nulo y φ un vector de S , diferente de 0. El subespacio (φ) engendrado por φ es un Δ -subgrupo de S , diferente de cero: luego coincide con S , ya que S es un Δ -grupo simple. S es, en efecto, un subespacio monógeno.

Consideremos un espacio vectorial E sobre un cuerpo Δ y un subespacio, (o Δ -subgrupo), H de E . El grupo cociente E/H es, como sabemos, un Δ -grupo, siendo el producto αX ($\alpha \in \Delta$, $X \in E/H$) la clase módulo H que contiene al vector αx , donde x es un vector de X (cap. VIII, § 1, teorema 3).

Teorema 3. — *El Δ -grupo cociente E/H es un espacio vectorial sobre Δ . Para demostrarlo, bastará establecer las igualdades (2), (3), (4):*

$$(2) \quad (\alpha + \beta)X = \alpha X + \beta X$$

$$(3) \quad \alpha(\beta X) = (\alpha\beta)X$$

$$(4) \quad \epsilon X = X$$

La clase $(\alpha + \beta)X$ contiene el vector $(\alpha + \beta)x$, donde $x \in X$, pero

$$(\alpha + \beta)x = \alpha x + \beta x$$

pertenecen a la suma de las clases que contienen αx , y βx , por consiguiente a $\alpha X + \beta X$, lo que prueba la igualdad (2). Una demostración análoga vale para las otras dos.

Según el primer teorema de isomorfismo, para que H sea subespacio maximal de E , es necesario y suficiente que E/H sea simple, o sea, según el teorema 2, que sea monógeno.

Definición. — En un espacio vectorial E sobre un cuerpo Δ , se dice que n elementos $a_1, a_2, \dots, a_n$ ($n \geq 1$) son *linealmente dependientes* si verifican una relación de la forma

$$\lambda_1 a_1 + \dots + \lambda_n a_n = 0$$

con los $\lambda_i \in \Delta$ no todos nulos.

Los elementos $a_1, \dots, a_n$ son, por el contrario, *linealmente independientes* si toda igualdad

$$\lambda_1 a_1 + \dots + \lambda_n a_n = 0 \quad (\lambda_i \in \Delta)$$

implica

$$\lambda_1 = \dots = \lambda_n = 0.$$

Un vector único a es linealmente independiente si es diferente del vector nulo, y sólo en este caso.

Cuando n vectores son linealmente dependientes, uno al menos de entre ellos es combinación lineal de los otros: se dice que depende linealmente de ellos.

Un subconjunto S de un espacio vectorial $\mathcal{E}$ se dice *independiente* (o *libre*) si, para toda parte finita $\{s_1, \dots, s_p\}$ sacada de S , los $s_1, \dots, s_p$ son en $\mathcal{E}$ elementos linealmente independientes. La familia $\mathfrak{I}$ de los subconjuntos independientes será no vacía en cuanto haya en $\mathcal{E}$ algún vector $v \neq 0$. Puesto que S viene caracterizada por una propiedad de carácter finito, la familia $\mathfrak{I}$ es $\mathbf{U}$ -inductiva (cap. VI, §1, 3.º). El axioma de Zorn implica pues, que para toda parte independiente S de $\mathcal{E}$, existe una parte maximal B que contiene a S .

Ahora bien, toda parte independiente maximal B es un sistema de generadores de $\mathcal{E}$. En efecto, si $x \in \mathcal{E} - B$, $B \cup \{x\}$ no es ya un subconjunto independiente. Además, todo subconjunto finito de elementos linealmente dependientes sacado de $B \cup \{x\}$ contiene necesariamente a x . Por consiguiente, x es combinación lineal de un número finito de elementos de B .

Existen pues, en todo espacio vectorial $\mathcal{E}$, sistemas de generadores independientes; estos sistemas son, por definición, las *bases* de $\mathcal{E}$; podemos enunciar el teorema siguiente.

Teorema 4. — *Todo espacio vectorial $\mathcal{E}$ admite al menos una base B , que contiene a un sistema independiente dado S .*

Si ahora se dan a la vez un subconjunto independiente S y una base cualquiera B_0 de $\mathcal{E}$, la familia (no vacía) de partes independientes X que verifican la limitación

$$S \subseteq X \subseteq S \cup B_0$$

es $\mathbf{U}$ -inductiva, luego contiene una parte maximal B' que es una base que contiene a S y que está contenida en $S \cup B_0$; en consecuencia:

Teorema 5. — *Todo subconjunto independiente S puede ser completado por vectores tomados en una base dada B_0 de forma que constituyan una base B' (teorema del cambio).*

Sean entonces $\mathcal{E}_1$ un subespacio de $\mathcal{E}$, B una base de $\mathcal{E}$, B_1 una base de $\mathcal{E}_1$. Completamos B_1 con un subconjunto de B de modo adecuado para formar una base B' de $\mathcal{E}$ que contenga a B_1 ; sea $\mathcal{E}_2$ el subespacio de $\mathcal{E}$ engendrado por $B_2 = B' - B_1$. Puesto que B_1 y B_2 son dos partes disjuntas de la base B' , $\mathcal{E}$ es la suma directa de los subespacios $\mathcal{E}_1$ y $\mathcal{E}_2$ engendrados por B_1 y B_2 :

$$\mathcal{E} = \mathcal{E}_1 \oplus \mathcal{E}_2.$$

Un tal espacio $\mathfrak{E}_2$ se llama *suplementario* de $\mathfrak{E}_1$; hemos obtenido el resultado siguiente.

Teorema 6. — *Para todo subespacio $\mathfrak{E}_1$ de un espacio vectorial $\mathfrak{E}$, existe al menos un suplementario $\mathfrak{E}_2$.*

Se puede también demostrar este teorema de la manera siguiente:

Supongamos $\mathfrak{E}_1$ subespacio *propio* de $\mathfrak{E}$ y sea ν un vector no nulo, que no pertenezca a $\mathfrak{E}_1$. Vistos como Δ -subgrupos, los subespacios de $\mathfrak{E}$ forman una familia $\mathbf{U}$ -inductiva $\mathcal{F}$; existe, pues, al menos un subespacio $\mathfrak{E}_2$ maximal entre los que contienen ν y cortan $\mathfrak{E}_1$ según $\mathfrak{E}_1 \cap (\nu) = (0)$ (cap. VI, §2, teorema 1). Resulta de ello que la suma $\mathfrak{E}_1 + \mathfrak{E}_2$ es *directa*:

$$\mathfrak{E}_1 \cap \mathfrak{E}_2 = (0), \quad \mathfrak{E}_1 + \mathfrak{E}_2 = \mathfrak{E}_1 \oplus \mathfrak{E}_2.$$

Mostremos que esta suma es $\mathfrak{E}$. En el caso contrario, existiría un vector x *no nulo* no perteneciente a $\mathfrak{E}_1 \oplus \mathfrak{E}_2$. El subespacio monógeno engendrado por x sería simple, luego $\mathfrak{E}_1 \oplus \mathfrak{E}_2$ cortaría a (x) en sólo el elemento 0. Por consiguiente, $(\mathfrak{E}_1 \oplus \mathfrak{E}_2) + (x)$ sería una suma directa contenida en $\mathfrak{E}$:

$$(\mathfrak{E}_1 \oplus \mathfrak{E}_2) + (x) = (\mathfrak{E}_1 \oplus \mathfrak{E}_2) \oplus (x) = \mathfrak{E}_1 \oplus [\mathfrak{E}_2 \oplus (x)]$$

lo que contradice que $\mathfrak{E}_2$ sea maximal.

En conclusión, *existe un suplementario $\mathfrak{E}_2$ de $\mathfrak{E}_1$, e incluso un suplementario que contiene a un vector dado no nulo ν si éste cumple la condición de no pertenecer a $\mathfrak{E}_1$.*

Observaciones. — Dado un subespacio propio $\mathfrak{E}_1$ de $\mathfrak{E}$, es necesario evitar el confundir un subespacio suplementario $\mathfrak{E}_2$, con el conjunto complementario C_1 de $\mathfrak{E}_1$ en $\mathfrak{E}$. Todo vector x de $\mathfrak{E}$ admite una representación única $x = x_1 + x_2$, con $x_i \in \mathfrak{E}_i$; $\mathfrak{E}_2$ es el conjunto de vectores cuya primera componente x_1 es nula; C_1 es el conjunto de vectores cuya segunda componente x_2 no es nula (no es un subespacio de $\mathfrak{E}$).

Se tendrá en cuenta también que un subespacio propio $\mathfrak{E}_1$ admite varios suplementarios distintos $\mathfrak{E}_2, \mathfrak{E}_2', \dots$. Si, en efecto, cambiamos el vector $\nu (\in \mathfrak{E}_2)$ de la demostración precedente por $\nu' = \nu + \nu_1$ ($\nu_1 \in \mathfrak{E}_1, \nu_1 \neq 0$), todo suplementario $\mathfrak{E}_2$ formado a partir de ν' es distinto de $\mathfrak{E}_2$ ya que $\nu' \notin \mathfrak{E}_2$.

Espacios vectoriales de base finita. — Para este caso vamos a encontrar otra vez, sin utilizar el axioma de Zorn, los teoremas precedentes, y los completaremos refiriéndolos a la teoría de grupos semisimples con un dominio de operadores.

Sea A un subespacio del espacio vectorial E . Supongamos que A admite una *base* (finita)

$$A = (a_1, a_2, \dots, a_n).$$

Esto quiere decir que todo vector $x \in A$ admite una representación

$$x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n \quad (\alpha_i \in \Delta).$$

Esta representación es *única* porque

$$x = \beta_1 a_1 + \beta_2 a_2 + \dots + \beta_n a_n$$

implica

$$(\alpha_1 - \beta_1)a_1 + \dots + (\alpha_n - \beta_n)a_n = 0$$

de donde, por ser los a_i linealmente independientes,

$$\alpha_i = \beta_i \quad (i = 1, \dots, n).$$

Inversamente, si un sistema de generadores $\{a_1, \dots, a_n\}$ de A es tal, que para todo elemento x de A la representación

$$x = \alpha_1 a_1 + \dots + \alpha_n a_n$$

es *única*, este sistema es una *base* de A , ya que

$$0 = \lambda_1 a_1 + \dots + \lambda_n a_n = 0a_1 + \dots + 0a_n$$

implica $\lambda_i = 0$ ($i = 1, \dots, n$).

Pero la unicidad de esta representación significa, ya que A es un grupo *abeliano*, que A es *suma directa* de los Δ -subgrupos *simples* $(a_1), \dots, (a_n)$:

$$A = (a_1) \oplus \dots \oplus (a_n)$$

luego, que A es un Δ -grupo *semisimple*. De este modo:

Teorema 7.—*Los espacios vectoriales (o los subespacios de un espacio vectorial) sobre un cuerpo Δ que admiten una base finita con n elementos, son los Δ -grupos (o los Δ -subgrupos) semisimples, sumas directas de n grupos simples.*

Ahora bien, hemos visto en el cap. VIII (§ 4) que el número n de factores

en todas las descomposiciones posibles de un grupo semisimple en factores simples es fijo. Este *invariante*, igual a la longitud de una serie de composición del grupo, es por definición, en el caso de los espacios vectoriales *la dimensión n del espacio*. Si un espacio vectorial A admite una base finita con n generadores, cualquier otra base de este espacio tendrá, igualmente, n generadores.

Si A es un espacio de dimensión n que admite la base $(a_1, \dots, a_n)$, tendremos para A la serie de composición de longitud n :

$$A = (a_1, \dots, a_n) \supset (a_1, \dots, a_{n-1}) \supset \dots \supset (a_1) \supset (0).$$

Recíprocamente, consideremos un espacio vectorial A sobre un cuerpo Δ y supongamos que admite una serie de composición de longitud n :

$$A = A_n \supset A_{n-1} \supset \dots \supset A_1 \supset A_0 = (0).$$

Cada uno de los espacios cociente A_i/A_{i-1} es simple, por lo tanto monógeno. En particular $A_1/(0) \simeq A_1$ es simple, por lo que A_1 admite una base de un solo elemento

$$A_1 = (a_1) \quad (a_1 \neq 0).$$

Razonemos entonces por recurrencia; supongamos establecido que A_{i-1} tiene una base de $i-1$ elementos

$$A_{i-1} = (a_1, \dots, a_{i-1}).$$

Tenemos $A_i/A_{i-1} = (V_i)$; si $x \in A_i$ y $x \notin A_{i-1}$, x está situado, en una clase X módulo A_{i-1} distinta de la clase cero, y tendremos

$$X = \alpha_i V_i \quad (\alpha_i \in \Delta, \alpha_i \neq 0)$$

de donde, volviendo a los vectores y llamando a_i a un representante de la clase V_i ,

$$\text{luego} \quad x = y + \alpha_i a_i \quad \text{con} \quad y \in A_{i-1}$$

$$\text{y} \quad y = \alpha_1 a_1 + \dots + \alpha_{i-1} a_{i-1}$$

$$x = \alpha_1 a_1 + \dots + \alpha_{i-1} a_{i-1} + \alpha_i a_i.$$

Se ve así que $\{a_1, \dots, a_{i-1}, a_i\}$ es un sistema de generadores de A_i .

Los vectores $a_1, \dots, a_{i-1}, a_i$ son *linealmente independientes*, pues, una relación de la forma

$$\lambda_1 a_1 + \dots + \lambda_{i-1} a_{i-1} + \lambda_i a_i = 0$$

implica, pasando a las clases de módulo A_{i-1} :

$$\lambda_i V_i = 0 \ (\in A_i/A_{i-1})$$

de donde $\lambda_i = 0$, y después $\lambda_1 = \dots = \lambda_{i-1} = 0$, ya que $a_1, \dots, a_{i-1}$ son independientes.

Cada uno de los espacios A_i posee pues una base de i elementos, en particular $A = A_n$ admite una base de n elementos, luego es de dimensión n .

Teorema 5. — *Los espacios vectoriales sobre Δ que admiten una base finita de n elementos (o de dimensión n) son los espacios vectoriales que admiten una serie de composición de longitud n .*

Sea $A = (a_1, \dots, a_n)$ un espacio vectorial de dimensión n sobre Δ . Por todo subespacio propio A' de A pasa una serie de composición (cap. VIII, § 3):

$$A = A_n \supset \dots \supset A_k = A' \supset \dots \supset A_0 = (0).$$

La parte de esta sucesión que va de $A' = A_k$ a (0) es una serie de composición de A' de longitud k : luego A' es de dimensión finita $k < n$.

Teorema 6. — *Todo subespacio propio de un espacio vectorial de dimensión n es de dimensión finita $k < n$.*

Corolario. — *En un espacio vectorial A de dimensión n , es imposible encontrar más de n vectores linealmente independientes.*

Sea $\{b_1, \dots, b_s\}$ un conjunto de s vectores de A linealmente independientes. Estos vectores engendran un subespacio $(b_1, \dots, b_s) = B$ de A de dimensión s . Según el teorema 6, tenemos $s \leq n$.

Obtenemos así una nueva definición de dimensión, cuando es finita: *la dimensión es el número máximo de vectores linealmente independientes.*

Sea $B = (b_1, \dots, b_s)$ un subespacio de dimensión s del espacio $A = (a_1, \dots, a_n)$, de dimensión n . Si se considera una serie de composición de A que pase por B , el razonamiento utilizado en la demostración del teorema 5

muestra que existe una base de A , formada de n vectores, incluyendo a los $b_1, \dots, b_s$:

$$A = (b_1, \dots, b_s, b_{s+1}, \dots, b_n)$$

(teorema de la complementación de la base).

Los $n-s$ vectores complementarios pueden, además, ser elegidos en una base $(a_1, \dots, a_n)$ de A dada a priori. Tenemos en efecto

$$A = (a_1) \oplus \dots \oplus (a_n)$$

y según el teorema general establecido en el capítulo VIII (§ 4, teorema 3), tenemos

$$\begin{aligned} A &= B \oplus (a_{i_1}) \oplus \dots \oplus (a_{i_{n-s}}) \\ &= (b_1) \oplus \dots \oplus (b_s) \oplus (a_{i_1}) \oplus \dots \oplus (a_{i_{n-s}}). \end{aligned}$$

De este modo, si hemos dado, por una parte, una base $(a_1, \dots, a_n)$ del espacio A , y por otra un sistema $(b_1, \dots, b_s)$ de s vectores independientes, ($s \leq n$), se puede formar una base de A con $b_1, \dots, b_s$ y $n-s$ vectores convenientes tomados entre los a_i (teorema del cambio, o teorema de Steinitz).

Si, con las notaciones precedentes, ponemos

$$B' = (b_{s+1}, \dots, b_n)$$

$$C = (a_{i_1}, \dots, a_{i_{n-s}})$$

tenemos

$$A = B \oplus B' = B \oplus C.$$

Al subespacio B de dimensión s , podemos pues asociar los subespacios $B', C, \dots$ de dimensión $n-s$, llamados suplementarios de B , tales que A sea suma directa de B y de un suplementario (teorema de la existencia de suplementario, en el caso de un espacio A de dimensión finita).

Si dos grupos G, G' son isomorfos y si uno de ellos, G , admite series de composición de longitud l , el otro G' admitirá series de composición de la misma longitud l . Resulta, pues, que, si dos espacios vectoriales E, E' sobre el cuerpo Δ son isomorfos (considerados como Δ -grupos), y si E es de dimensión finita n , entonces E' es también de dimensión n .

Recíprocamente, dos espacios E, F de la misma dimensión n , sobre el mismo cuerpo Δ son isomorfos (como Δ -grupos); tomemos en efecto una base para cada uno de ellos:

$$E = (a_1, \dots, a_n), \quad F = (b_1, \dots, b_n);$$

la aplicación

$$x = \sum_{i=1}^n \lambda_i a_i \rightarrow y = \sum_{i=1}^n \lambda_i b_i$$

de E sobre F es visiblemente un Δ -isomorfismo.

Sea ahora B un subespacio de dimensión s en un espacio vectorial A de dimensión n . Designando por B' un suplementario de B , de dimensión $n - s$, la igualdad

$$A = B \oplus B'$$

implica

$$A/B \simeq B'.$$

Luego, el espacio cociente de un espacio de dimensión n por un subespacio de dimensión s es un espacio vectorial de dimensión $n - s$.

Consideremos finalmente, en un espacio vectorial E (de dimensión finita o infinita), dos subespacios H y K de dimensiones finitas, que designamos por $\dim H = h$ y $\dim K = k$, respectivamente. Sean $S = H + K$, $I = H \cap K$ la suma y la intersección de H y K . La reunión de una base de H y de una base de K es un sistema de generadores para S , y en este sistema finito hay evidentemente subconjuntos maximales de vectores linealmente independientes, que son bases de S . S es pues un espacio de dimensión finita s , con $s \leq h + k$. Sea i la dimensión de I . Tenemos, según el segundo teorema de isomorfismo

$$(H + K)/H \simeq K/(H \cap K)$$

esto es,

$$S/H \simeq K/I$$

de donde, ya que dos espacios isomorfos tienen la misma dimensión,

$$s - h = k - i \quad \text{o} \quad i + s = h + k.$$

es decir

$$\dim (H + K) = \dim H + \dim K - \dim (H \cap K)$$

§ 2. Aplicaciones lineales y matrices

Definición. — Consideremos dos espacios vectoriales $\mathfrak{E}$ y $\mathfrak{E}'$, sobre un mismo cuerpo conmutativo Δ , y los Δ -homomorfismos de $\mathfrak{E}$ en $\mathfrak{E}'$ que llamaremos *apli-*

caciones lineales de $\mathfrak{E}$ en $\mathfrak{E}'$. A todo $x \in \mathfrak{E}$ viene asociado por el homomorfismo α un vector $\alpha x = y$ de $\mathfrak{E}'$, y sólo uno, de forma que

$$(1) \quad \begin{aligned} \alpha(x_1 + x_2) &= \alpha x_1 + \alpha x_2 \\ \alpha(\lambda x) &= \lambda(\alpha x), \quad \forall \lambda \in \Delta. \end{aligned}$$

Ejemplo. — En el espacio $\mathfrak{E}_3$, una proyección, una homotecia, son aplicaciones lineales.

Definimos que dos aplicaciones α y β de $\mathfrak{E}$ en $\mathfrak{E}'$ son *iguales* si tienen el mismo efecto sobre todo vector x de $\mathfrak{E}$: $\alpha x = \beta x$, $\forall x \in \mathfrak{E}$.

Observación. — De la definición de aplicaciones lineales (fórmulas (1)), resulta:

$$\alpha(\lambda_1 x_1 + \dots + \lambda_n x_n) = \lambda_1(\alpha x_1) + \dots + \lambda_n(\alpha x_n).$$

Por lo tanto: *Las imágenes de vectores linealmente dependientes son también vectores linealmente dependientes.*

Consideremos un tercer espacio $\mathfrak{E}''$ y una aplicación lineal α' de $\mathfrak{E}'$ en $\mathfrak{E}''$; al vector x de $\mathfrak{E}$, α asocia un vector $y = \alpha x$ de $\mathfrak{E}'$; pero a este vector y , α' asocia un vector $\alpha' y = z$ de $\mathfrak{E}''$. Se tiene pues una aplicación $\varpi = \alpha' \circ \alpha$, $x \rightarrow z$, de $\mathfrak{E}$ en $\mathfrak{E}''$; mostremos que también es una aplicación lineal.

Es necesario demostrar ante todo que:

$$\varpi(x_1 + x_2) = \varpi x_1 + \varpi x_2$$

Ahora bien, se tiene

$$\alpha'[\alpha(x_1 + x_2)] = \alpha'[y_1 + y_2] = \alpha' y_1 + \alpha' y_2 = z_1 + z_2$$

donde hemos puesto:

$$z_i = \alpha' y_i \quad \text{y} \quad y_i = \alpha x_i.$$

Ahora es necesario demostrar que:

$$\varpi(\lambda x) = \lambda(\varpi x);$$

y en efecto:

$$\varpi(\lambda x) = \alpha'(\alpha \lambda x) = \alpha'(\lambda y) = \lambda(\alpha' y) = \lambda z = \lambda(\varpi x).$$

Para simplificar la notación, escribiremos $\varpi = \alpha' \alpha$ y diremos que ϖ es el *producto* de α por α' ; el factor *de la derecha* α , es la aplicación que se realiza *primero*.

El producto de aplicaciones lineales así definido es una ley de composición general sobre los tres conjuntos siguientes:

A , conjunto de aplicaciones de $\mathfrak{E}$ en $\mathfrak{E}'$,

B , conjunto de aplicaciones de $\mathfrak{E}'$ en $\mathfrak{E}''$,

C , conjunto de aplicaciones de $\mathfrak{E}$ en $\mathfrak{E}''$.

En el conjunto A , vamos a definir ahora una ley de composición interna que llamaremos *adición*.

Consideremos en A dos aplicaciones lineales α_1 y α_2 (de $\mathfrak{E}$ en $\mathfrak{E}'$). Si x es un vector cualquiera de $\mathfrak{E}$, ponemos

$$\alpha_1 x = y_1, \quad \alpha_2 x = y_2, \quad y_1, y_2 \in \mathfrak{E}'.$$

Pero, por ser $\mathfrak{E}'$ un espacio vectorial, se puede formar:

$$s = y_1 + y_2 \in \mathfrak{E}'$$

y la aplicación σ que hace pasar de $x \in \mathfrak{E}$ a $s \in \mathfrak{E}'$ es una aplicación lineal. En efecto, por definición

$$\sigma x = \alpha_1 x + \alpha_2 x.$$

Formemos:

$$\sigma(x + x'), \quad x, x' \in \mathfrak{E}.$$

Tenemos:

$$\sigma(x + x') = \alpha_1(x + x') + \alpha_2(x + x') = \alpha_1 x + \alpha_1 x' + \alpha_2 x + \alpha_2 x'$$

siendo α_1 y α_2 aplicaciones lineales, de donde

$$\sigma(x + x') = \alpha_1 x + \alpha_2 x + \alpha_1 x' + \alpha_2 x'$$

a causa de la conmutatividad, y en fin

$$\sigma(x + x') = \sigma x + \sigma x'.$$

Si se multiplica por un escalar, se tiene sucesivamente

$$\begin{aligned} \sigma(\lambda x) &= \alpha_1(\lambda x) + \alpha_2(\lambda x) \\ &= \lambda(\alpha_1 x) + \lambda(\alpha_2 x) \\ &= \lambda(\alpha_1 x + \alpha_2 x) \\ &= \lambda(\sigma x) \quad \forall \lambda \in \Delta. \end{aligned}$$

Esta operación $\sigma = a_1 + a_2$ es asociativa y conmutativa. Por otra parte, existe una aplicación θ que va a jugar el papel de elemento neutro; es la que asocia a todo $x \in \mathfrak{E}$ el vector nulo, 0, de $\mathfrak{E}'$, pues, si se la adiciona con una aplicación cualquiera α , se tendrá $\alpha + \theta = \alpha$, ya que

$$(\alpha + \theta)x = \alpha x + \theta x, \quad \text{con} \quad \theta x = 0.$$

Finalmente, para toda aplicación α , existe una aplicación $-\alpha$, que asocia a x el vector opuesto a αx , y la suma de α y $-\alpha$ da la aplicación nula θ : $\alpha + (-\alpha) = \theta$.

Luego las aplicaciones lineales de $\mathfrak{E}$ en $\mathfrak{E}'$ forman un grupo aditivo.

Caso particular $\mathfrak{E}' = \mathfrak{E}$.—Nos ocuparemos particularmente de las aplicaciones lineales de $\mathfrak{E}$ en sí mismo. Podemos entonces definir la adición y la multiplicación de dos aplicaciones lineales tomadas ambas en el mismo conjunto, el conjunto $\mathcal{A}$ de las aplicaciones lineales de $\mathfrak{E}$ en $\mathfrak{E}$.

Según lo que precede, $\mathcal{A}$ es un grupo abeliano aditivo. En cuanto a la multiplicación, es asociativa, por consiguiente $\mathcal{A}$ es un semigrupo multiplicativo. Demostremos que la multiplicación es distributiva, respecto a la adición: resultará que $\mathcal{A}$ es un anillo.

Consideremos las aplicaciones lineales α , α_1 y β de $\mathfrak{E}$ en sí mismo.

Tenemos, en primer lugar

$$(1) \quad (\alpha + \alpha_1)\beta = \alpha\beta + \alpha_1\beta.$$

En efecto:

$$\begin{aligned} [(\alpha + \alpha_1)\beta]x &= (\alpha + \alpha_1)(\beta x) = \alpha(\beta x) + \alpha_1(\beta x) \\ &= (\alpha\beta)x + (\alpha_1\beta)x = (\alpha\beta + \alpha_1\beta)x. \end{aligned}$$

Los dos miembros de (1) tienen el mismo efecto sobre un elemento cualquiera x de $\mathfrak{E}$ y, en consecuencia, la igualdad (1) queda establecida.

Establezcamos ahora la propiedad distributiva a izquierda:

$$(1') \quad \beta(\alpha + \alpha_1) = \beta\alpha + \beta\alpha_1.$$

Tenemos

$$\begin{aligned} [\beta(\alpha + \alpha_1)]x &= \beta[(\alpha + \alpha_1)x] = \beta[\alpha x + \alpha_1 x] \\ &= \beta(\alpha x) + \beta(\alpha_1 x) = (\beta\alpha)x + (\beta\alpha_1)x \\ &= (\beta\alpha + \beta\alpha_1)x. \end{aligned}$$

y esto para todo $x \in \mathfrak{E}$, lo que equivale a la igualdad (1').

Propiedades del anillo $\mathcal{A}$. — *En general no es conmutativo.* En efecto, si tomamos como espacio vectorial el espacio vectorial ordinario $\mathfrak{E}_3$ de tres dimensiones, tenemos entre las aplicaciones lineales los movimientos que dejan un punto O fijo, y se sabe que su multiplicación no es conmutativa.

El anillo $\mathcal{A}$ tiene elemento unidad, la aplicación idéntica, que designaremos por I :

$$Ix = x, \quad \forall x \in \mathfrak{E};$$

si se multiplica I por a , se tiene:

$$aI = Ia = a.$$

El anillo $\mathcal{A}$ admite también, para $n \geq 2$, verdaderos divisores de cero. Para constatarlo, sea en nuestro espacio $\mathfrak{E}$ un subespacio propio $\mathfrak{E}_1$.

$$0 \subset \mathfrak{E}_1 \subset \mathfrak{E}.$$

Este subespacio admite un suplementario $\mathfrak{E}_2$, $\mathfrak{E} = \mathfrak{E}_1 \oplus \mathfrak{E}_2$. Cualquiera sea $x \in \mathfrak{E}$, se le puede expresar de un modo y de uno sólo, en la forma:

$$x = x_1 + x_2, \quad x_1 \in \mathfrak{E}_1, \quad x_2 \in \mathfrak{E}_2.$$

Consideremos la aplicación α_1 que a x asocia $x_1 \in \mathfrak{E}_1$, perfectamente definida; α_1 cumple evidentemente la primera condición para ser lineal; e igualmente la segunda, pues si λ es un elemento cualquiera del cuerpo base Δ se tiene:

$$\lambda x = \lambda x_1 + \lambda x_2.$$

Ahora bien, $\lambda x_1 \in \mathfrak{E}_1$, luego λx_1 es la componente de λx en $\mathfrak{E}_1$. Así, α_1 es una aplicación lineal; otro tanto vale para α_2 , que a x asocia x_2 . Estas dos aplicaciones son distintas de θ , porque si se aplica α_1 a un vector no nulo v_1 , de $\mathfrak{E}_1$, se obtiene $\alpha_1 v_1 = v_1 \neq 0$; lo mismo es el razonamiento para α_2 .

Llamaremos a α_1 y α_2 las proyecciones de $\mathfrak{E}$ sobre $\mathfrak{E}_1$ y sobre $\mathfrak{E}_2$, respectivamente. Como se ve inmediatamente, son aplicaciones idempotentes.

Estas aplicaciones α_1 , α_2 son divisores de cero, porque se tiene:

$$\alpha_1 \alpha_2 = \alpha_2 \alpha_1 = \theta.$$

En efecto:

$$\begin{aligned} (\alpha_1 \alpha_2)x &= \alpha_1(\alpha_2 x) & (x \in \mathfrak{E}) \\ &= \alpha_1 x_2, \end{aligned}$$

Ahora bien, $x_2 = 0 + x_2$; su componente en $\mathcal{E}_1$ es nula; luego

$$(a_1 a_2)x = 0, \quad \forall x \in \mathcal{E},$$

es decir

$$a_1 a_2 = \theta.$$

Matrices. — Consideremos las aplicaciones lineales de un espacio vectorial $\mathcal{E}$ de dimensión finita n en un espacio vectorial $\mathcal{E}'$ de dimensión finita p . Vamos a pasar de la noción de aplicación lineal a la noción de matriz tomando, para ello, sendas bases de dichos espacios:

$$\mathcal{E} = (e_1, \dots, e_n), \quad \mathcal{E}' = (e'_1, \dots, e'_p).$$

Si consideramos la aplicación lineal α de $\mathcal{E}$ en $\mathcal{E}'$, es natural llevar nuestra atención a las imágenes de los elementos de la base de $\mathcal{E}$, es decir, a los vectores:

$$\alpha e_k = t_k \in \mathcal{E}',$$

los cuales engendran el llamado *espacio imagen* $\alpha\mathcal{E}$:

$$\alpha\mathcal{E} = (t_1, \dots, t_n).$$

La dimensión de este espacio es $\leq n$; por otra parte, como $\alpha\mathcal{E}$ es un subespacio de $\mathcal{E}'$, es también $\leq p$, luego

$$\text{dimensión } \alpha\mathcal{E} \leq \inf(n, p).$$

Veamos, en particular, que si $p < n$ la dimensión de $\alpha\mathcal{E}$ es $< n$, y por consiguiente los vectores t_k son linealmente dependientes. Si $p \geq n$, esta limitación no existe ya y la dimensión del espacio imagen $\alpha\mathcal{E}$ será n si, y sólo si, los vectores t_k son linealmente independientes.

Sentado eso, los vectores t_k del espacio $\mathcal{E}'$ pueden expresarse por medio de la base $e'_1, \dots, e'_p$:

$$\alpha e_k = t_k = \sum_i a_{ik} e'_i \quad (i = 1, \dots, p; k = 1, \dots, n).$$

Tenemos pues np elementos a_{ik} de Δ que son las *coordenadas de los vectores* $\alpha e_k = t_k$ de $\mathcal{E}'$. Conviene ordenar estos np números a_{ik} en un *cuadro rec-*

tangular de p filas y n columnas:

$$\begin{pmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ a_{21} & \dots & a_{2k} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ik} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{p1} & \dots & a_{pk} & \dots & a_{pn} \end{pmatrix}, \quad a_{ik} \in \Delta$$

En la columna de orden k (o, simplemente, columna k) figuran las coordenadas $a_{1k}, \dots, a_{pk}$ del vector t_k .

Este cuadro es, por definición, la *matriz de la aplicación lineal* α cuando los espacios vectoriales $\mathcal{E}$ y $\mathcal{E}'$ están definidos por las bases en cuestión.

Designaremos esa matriz por la letra A , y escribiremos:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{p1} & \dots & a_{pn} \end{pmatrix} = \| a_{ik} \|$$

Una matriz con p filas y n columnas se dice de tipo $p \times n$, o se le llama, simplemente *matriz* $p \times n$.

Observación. — Una matriz no sólo depende de la aplicación lineal que representa, sino también de las bases escogidas en los dos espacios vectoriales considerados.

Fijadas las bases en $\mathcal{E}$ y $\mathcal{E}'$, el conocimiento de la matriz A de una aplicación lineal α determina completamente esta aplicación, es decir, que dada A , se sabe encontrar la imagen, en la aplicación α , de un vector cualquiera x de $\mathcal{E}$. En efecto, sea

$$x = \sum_k \xi_k e_k, \quad \xi_k \in \Delta$$

Se tiene entonces

$$\begin{aligned} \alpha x &= \sum_k \xi_k \alpha e_k = \sum_k \xi_k \left(\sum_i a_{ik} e'_i \right) \\ &= \sum_i \left(\sum_k a_{ik} \xi_k \right) e'_i = \sum_i \xi'_i e'_i; \end{aligned}$$

obtenemos con ello las coordenadas ξ'_i del vector transformado:

$$\xi'_i = \sum_k a_{ik} \xi_k$$

Tenemos de este modo, al dejar fijos los dos espacios y sus bases, un conjunto $\mathcal{M}$ de matrices A correspondiente al conjunto $\mathcal{A}$ de las aplicaciones lineales α .

Igualdad. — Se dice que dos matrices A y B son iguales, cuando las aplicaciones lineales α y β de que provienen lo son:

$$\alpha x = \beta x, \quad \forall x \in \mathcal{E}.$$

Para esto, es necesario y suficiente que el efecto de α y de β sobre cada vector fundamental sea el mismo:

$$\alpha e_k = \beta e_k, \quad \forall k (= 1, 2, \dots, n)$$

o también, que estos vectores tengan las mismas coordenadas:

$$a_{ik} = b_{ik}, \quad \forall i, k \in \{1, 2, \dots, n\}.$$

Para que dos matrices sean iguales, es decir, para que representen con las mismas bases, aplicaciones lineales iguales, es necesario y suficiente que los elementos homólogos (de índices iguales) sean iguales.

Con esta definición de igualdad de matrices, vemos que hay correspondencia biyectiva entre el conjunto de aplicaciones lineales y el conjunto de matrices que las representan en bases fijas.

$$\alpha \longleftrightarrow A.$$

Adición. — Hemos definido para las aplicaciones lineales una adición poniendo

$$(\alpha + \beta)x = \alpha x + \beta x, \quad \forall x \in \mathcal{E}$$

en particular

$$(\alpha + \beta)e_k = \alpha e_k + \beta e_k,$$

de manera que el vector cuyas coordenadas constituyen la columna k de la matriz $\alpha + \beta$ es la suma de los vectores que constituyen las columnas k de la matriz que representa α y la que representa β . Estos vectores se adicionan coordenada a coordenada y, por consiguiente, si S es la matriz que representa $\alpha + \beta$, tenemos para el elemento genral s_{ik} de S :

$$s_{ik} = a_{ik} + b_{ik}.$$

Así hemos definido una *adición de matrices*, que se realiza sumando elemento a elemento, cada uno con su homólogo.

La aplicación nula θ , tal que $\theta e_k = 0$, tiene por matriz la *matriz nula*, en la cual todos los elementos son cero:

$$0 = \begin{vmatrix} 0 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 0 \end{vmatrix}$$

La matriz de la aplicación $-a$ opuesta a a es la *matriz $-A$ opuesta a A* ; tiene sus elementos opuestos a los de A :

$$-A = \parallel -a_{ij} \parallel$$

Con todo esto, el conjunto $\mathcal{M}$ de matrices $n \times p$ es manifiestamente un grupo abeliano aditivo.

Multiplicación. — Con los dos espacios

$$\mathcal{E} = (e_1, \dots, e_n) \quad \text{y} \quad \mathcal{E}' = (e'_1, \dots, e'_p)$$

consideremos un tercer espacio $\mathcal{E}'' = (e''_1, \dots, e''_q)$, una aplicación de $\mathcal{E}$ en $\mathcal{E}'$ y una aplicación a' de $\mathcal{E}'$ en $\mathcal{E}''$; su producto $a'a$ es una aplicación de $\mathcal{E}$ en $\mathcal{E}''$; Busquemos su matriz, que será de q filas y n columnas. Para ello, transformemos los vectores de la base:

$$a''e_k = \sum_i p_{ik} e''_i;$$

ahora bien

$$\begin{aligned} a''e_k &= a'a e_k = a' \left(\sum_{\lambda} a_{\lambda k} e'_{\lambda} \right) \\ &= \sum_{\lambda} a_{\lambda k} a' e'_{\lambda} = \sum_{\lambda} a_{\lambda k} \sum_i a'_{i\lambda} e''_i = \sum_i \left(\sum_{\lambda} a'_{i\lambda} a_{\lambda k} \right) e''_i \end{aligned}$$

de donde, para la matriz producto $P = A'A$:

$$p_{ik} = \sum_{\lambda=1}^p a'_{i\lambda} a_{\lambda k}$$

Es decir: *Las matrices se multiplican filas por columnas*; p_{ik} es la suma de los productos de los elementos de la fila i de A' por los elementos del mismo lugar en la columna k de A .

Para las matrices, *la multiplicación es asociativa y distributiva respecto a la adición, ya que estas propiedades se cumplen para las aplicaciones lineales.*

Observaciones. — 1. Con frecuencia se llama vectores a las filas y las columnas de una matriz. Se habla así de *vectores filas* y de *vectores columnas*.

2. En un producto de matrices, el número de columnas de la matriz de la izquierda debe ser igual al número de filas de la de la derecha:

$$\text{matriz } n \times p \cdot \text{matriz } p \times q = \text{matriz } n \times q.$$

3. Tratamos hasta ahora de matrices que representan aplicaciones lineales. Los elementos de estas matrices pertenecen a un cierto cuerpo Δ sobre el cual formamos los oportunos espacios vectoriales.

Pero *a posteriori* se ve que hemos utilizado solamente la igualdad de elementos, su adición y su multiplicación. Por consiguiente, siempre que se dé un anillo conmutativo R , se pueden formar *a priori*, con los elementos de R , matrices satisfaciendo a las reglas precedentes de igualdad, adición y multiplicación. Pero entonces, la significación geométrica desaparece, y es preciso verificar mediante el cálculo las propiedades fundamentales de las operaciones a partir de las fórmulas:

$$\begin{aligned} s_{ik} &= a_{ik} + b_{ik} \\ p_{ik} &= \sum_{\lambda} a_{i\lambda} b_{\lambda k} \end{aligned}$$

lo cual no presenta dificultad.

Caso particular $\mathcal{E} = \mathcal{E}'$. — Volvamos al caso de un solo espacio vectorial en el que se toma una base única, $\mathcal{E} = (e_1, \dots, e_n)$. Consideremos el conjunto $\mathcal{A}$ de las aplicaciones lineales α de $\mathcal{E}$ en sí mismo: a cada una de estas aplicaciones α corresponde una matriz $A = \| a_{ik} \|$, con

$$\alpha e_k = t_k = \sum_i a_{ik} e_i,$$

matriz cuadrada de n filas y n columnas, cuyos elementos pertenecen al cuerpo de base Δ .

Se pueden aplicar las reglas de adición y de multiplicación precedentes. Hay correspondencia biunívoca entre $\mathcal{A}$ y el conjunto $\mathcal{M}$ de matrices:

$$\mathcal{A} \longleftrightarrow \mathcal{M}$$

y de acuerdo con la definición de operaciones con las matrices esta correspondencia respeta la adición y la multiplicación, de modo que $\mathcal{A}$ y $\mathcal{M}$ son isomorfos con relación a estas dos operaciones. Y como $\mathcal{A}$ es un anillo, también $\mathcal{M}$ es un anillo.

Las matrices cuadradas de orden n con elementos de un cuerpo Δ forman un anillo $\mathcal{M}$ con elemento unidad: la matriz unidad es la que representa la aplicación unidad o idéntica I

$$Ie_k = e_k.$$

La columna k de la matriz unidad es pues $0, 0 \dots 1, 0, \dots 0$, donde el elemento unidad de Δ , 1 , figura en el lugar k , y la matriz se escribe:

$$I = \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{vmatrix}$$

Si en lugar de operar sobre un espacio vectorial con matrices cuyos elementos pertenezcan a un cuerpo, se toman *a priori* matrices cuadradas de orden n con elementos de un anillo R , la asociatividad de la multiplicación y su propiedad distributiva respecto a la suma permanecen válidas. Por consiguiente, las matrices cuadradas de orden n con elementos de un anillo R también constituyen un anillo.

Se llaman *símbolos de Kronecker* los elementos

$$\delta_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases} \quad (i, j = 1, 2 \dots n)$$

o más generalmente, si se trabaja sobre un cuerpo abstracto cualquiera, del cual e es el elemento unidad, $\delta_{ij} = e \in \Delta$ para $i = j$, $\delta_{ij} = 0 \in \Delta$ para $i \neq j$.

Esta notación permite escribir la matriz unidad bajo la forma:

$$I = \parallel \delta_{ij} \parallel$$

Matrices escalares. Centro del anillo de las matrices cuadradas de orden n . Se llama matriz escalar una matriz de la forma

$$kI = \begin{vmatrix} k & 0 & \dots & 0 \\ 0 & k & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & k \end{vmatrix} \quad (k \in \Delta)$$

Dicha matriz se indica frecuentemente por el símbolo k .

Si se multiplica una matriz escalar por una matriz cualquiera $A = \| a_{ij} \|$, se obtiene:

$$kI \cdot A = kA = \| ka_{ij} \| = A \cdot kI.$$

De suerte que *toda matriz escalar kI es permutable con cualquier matriz A .*

Como en teoría de grupos, se llama *centro de un anillo* el conjunto de elementos del anillo que, para la multiplicación, son permutables con todos los del anillo.

Designemos por Z el centro del anillo de las matrices cuadradas de orden n sobre Δ . Toda matriz escalar pertenece al centro Z . Además:

Teorema. — *El centro del anillo de las matrices cuadradas de orden n se compone únicamente de las matrices escalares.*

Demostración. — Entre las matrices del anillo, consideremos la matriz E_{rs} cuyos elementos son ceros, excepto el de intersección de la fila r con la columna s , donde se encuentra el elemento-unidad:

$$E_{rs} = \begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & e & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix} \begin{matrix} \rightarrow \text{fila de orden } r \\ \downarrow \\ \text{columna de orden } s \end{matrix}$$

Una matriz cualquiera puede expresarse como combinación lineal de matrices E_{rs} :

$$(1) \quad A = \| a_{ij} \| = \sum_{i,j} a_{ij} E_{ij},$$

de manera que las n^2 matrices E_{rs} constituyen un sistema de generadores para el conjunto de las matrices del anillo. Además estos generadores son independientes, pues la igualdad

$$\sum_{ij} a_{ij} E_{ij} = 0,$$

en la que el primer miembro es la matriz A , significa $a_{ij} = 0, \forall i, j$.

Vemos pues, que las matrices cuadradas de orden n con elementos de un cuerpo Δ constituyen un espacio vectorial sobre Δ que admite como base las n -matrices E_{rs} . Luego este espacio vectorial es de dimensión n^2 ; además, es un anillo y, por consiguiente, una álgebra asociativa.

Utilizando la representación (1) de una matriz cualquiera mediante las matrices E_{ij} , es fácil demostrar que el centro Z es el conjunto de las matrices escalares. En efecto, para que una matriz sea conmutativa con todas las otras, es necesario en particular que sea conmutativa con cada una de las matrices E_{rs} . Calculemos $E_{pq}E_{rs}$; se tiene inmediatamente:

$$\begin{cases} E_{pq}E_{rs} = 0 & \text{si } q \neq r \\ E_{pq}E_{rs} = E_{ps} & \text{si } q = r \end{cases}$$

Ahora bien, utilizando la representación (1), tenemos

$$\begin{aligned} AE_{rs} &= \sum_{ij} a_{ij}E_{ij}E_{rs} = \sum_i a_{ir}E_{is} = \begin{vmatrix} 0 & \dots & \overset{\substack{\downarrow \text{columna de orden } s}}{a_{1r}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & a_{nr} & \dots & 0 \end{vmatrix} \\ E_{rs}A &= \sum_{ij} E_{rs}a_{ij}E_{ij} = \sum_j a_{sj}E_{rj} = \begin{vmatrix} 0 & \dots & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{s1} & \dots & \dots & \dots & a_{sn} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & \dots & 0 \end{vmatrix} \leftarrow \text{fila de orden } r \end{aligned}$$

y la igualdad $AE_{rs} = E_{rs}A$ exige:

$$a_{ir} = 0 \quad \text{para } i \neq r, \quad a_{rr} = a_{ss}, \quad \forall r, s \in \{1, 2, \dots, n\}$$

lo que expresa que A es una matriz escalar.

Otra demostración. — Sea ζ una aplicación lineal de $\mathfrak{E}$ en $\mathfrak{E}$ conmutativa con cualquiera otra,

$$\zeta a = a\zeta \quad \forall a \in \mathcal{A}.$$

Señalemos en primer lugar que si φ es un vector cualquiera de $\mathfrak{E}$, $\zeta\varphi = \varphi'$ no es linealmente independiente de φ ; si $\mathfrak{E}$ es de dimensión 1, ello es evidente.

Si $\mathcal{E}$ es de dimensión superior a 1 y si se suponen v y v' linealmente independientes, puede siempre encontrarse una aplicación lineal α tal que:

$$\alpha v = 0 \quad \text{y} \quad \alpha v' \neq 0.$$

En efecto, tomemos en $\mathcal{E}$ una base cuyos dos primeros elementos sean v y v' linealmente independientes; una aplicación lineal α está definida por las imágenes de los elementos de la base y puede darse para v una imagen nula y para v' una imagen no nula. Entonces, si se forma $\zeta\alpha$ y $\alpha\zeta$ y si se las aplica a v , se tiene:

$$\zeta\alpha v = \zeta(\alpha v) = \zeta 0 = 0,$$

mientras que

$$\alpha\zeta v = \alpha v' \neq 0,$$

luego

$$\zeta\alpha \neq \alpha\zeta \quad \text{y} \quad \zeta \notin Z,$$

contrariamente a la hipótesis.

Es, pues, imposible que ζv sea linealmente independiente de v :

$$\forall v \in \mathcal{E}, \quad \zeta v = kv,$$

dependiendo k *a priori* de v . Vamos a demostrar, que k es una constante. Apliquemos ζ a dos vectores v_1 y v_2 de $\mathcal{E}$:

$$\zeta v_1 = k_1 v_1, \quad \zeta v_2 = k_2 v_2.$$

1.º Si v_1 y v_2 son linealmente independientes, tendremos

$$\zeta(v_1 + v_2) = k_3(v_1 + v_2)$$

pero también

$$\zeta(v_1 + v_2) = \zeta v_1 + \zeta v_2 = k_1 v_1 + k_2 v_2$$

y la igualdad

$$k_3(v_1 + v_2) = k_1 v_1 + k_2 v_2,$$

donde v_1 y v_2 son linealmente independientes, exige

$$k_1 = k_3 \quad \text{y} \quad k_2 = k_3,$$

luego $k_1 = k_2$.

2.º Si v_1 y v_2 son linealmente dependientes, se tiene $v_2 = mv_1$, de donde

$$k_2 v_2 = \zeta v_2 = \zeta(mv_1) = m\zeta v_1 = mk_1 v_1 = k_1 v_2$$

luego también

$$k_1 = k_2.$$

3.º Para $v = 0$, k es indeterminado, convendremos en tomar el valor precedente. ζ es efectivamente una aplicación escalar u homotecia.

§ 3. Dimensión del espacio imagen. Aplicaciones lineales y matrices regulares o singulares

Sean $\mathcal{E}$ y $\mathcal{E}'$ dos espacios vectoriales sobre un mismo cuerpo (conmutativo) Δ , de dimensiones respectivamente n y p . Consideremos una aplicación lineal de $\mathcal{E}$ en $\mathcal{E}'$. Sea

$$\alpha(\mathcal{E}) = \mathcal{F} \subseteq \mathcal{E}'$$

el *espacio imagen* de $\mathcal{E}$, conjunto de los vectores imágenes $\alpha(x)$ de los vectores x de $\mathcal{E}$.

Puesto que α es un Δ -homomorfismo que aplica $\mathcal{E}$ sobre $\mathcal{F}$, tenemos, según el teorema de homomorfismo (cap. VIII, § 1, teor. 4), el isomorfismo:

$$(1) \quad \mathcal{F} \simeq \mathcal{E}/\mathcal{N}$$

donde $\mathcal{N}$, núcleo del homomorfismo α , es el conjunto de los vectores x cuya imagen $\alpha(x)$ es el vector nulo de $\mathcal{E}'$.

Además, el subespacio $\mathcal{N}$ admite al menos un suplementario $\mathcal{C}$,

$$\mathcal{E} = \mathcal{N} \oplus \mathcal{C},$$

y se tiene:

$$(2) \quad \mathcal{F} \simeq \mathcal{E}/\mathcal{N} \simeq \mathcal{C}.$$

Como dos espacios isomorfos tienen la misma dimensión, (2) implica, poniendo $\nu = \dim \mathcal{N}$ (dimensión de $\mathcal{N}$), $r = \dim \mathcal{F}$:

$$r = n - \nu = \dim \mathcal{C}.$$

Definición. — La dimensión r del espacio imagen $\mathcal{F} = \alpha(\mathcal{E})$ es el *rango* de la aplicación lineal α .

Corolario. — Para que la dimensión de $\mathcal{F} = \alpha(\mathcal{E})$ sea igual a la dimensión de $\mathcal{E}$, o, dicho de otro modo, para que α sea un isomorfismo de $\mathcal{E}$ sobre $\mathcal{F}$, es necesario que $v = 0$, es decir que el núcleo $\mathcal{N}$ se reduzca al vector cero; para que α sea un isomorfismo de $\mathcal{E}$ con $\mathcal{E}'$, es necesario y suficiente que r , n y p sean iguales.

Caso particular : $\mathcal{E} = \mathcal{E}'$.

Los isomorfismos toman entonces el nombre de *automorfismos*. Para que una aplicación lineal de $\mathcal{E}$ en sí mismo sea un automorfismo, es necesario y suficiente que su núcleo se reduzca al vector cero, o también que $r = n$. Pero para que $r = n$, es necesario y suficiente que $\alpha(\mathcal{E}) = \mathcal{E}$ y para eso es necesario y suficiente que los n vectores $\alpha(e_k)$ imágenes de los vectores fundamentales engendren todo el espacio, es decir, que sean *linealmente independientes*. Tenemos entonces toda una serie de propiedades equivalentes:

- la aplicación lineal α de $\mathcal{E}$ en sí mismo es un automorfismo,
- su núcleo $\mathcal{N}$ se reduce al vector nulo: $\alpha(x) = 0$ implica $x = 0$.
- $\alpha(\mathcal{E}) = \mathcal{E}$,
- los n vectores $\alpha(e_k)$ son linealmente independientes.

Se expresa una cualquiera de estas propiedades diciendo que la aplicación α es *regular*. Cuando una aplicación no sea regular, se llamará *singular*.

El conjunto de las aplicaciones regulares de $\mathcal{E}$ en sí mismo es un grupo respecto a la multiplicación (o composición) de estas aplicaciones. Es, en efecto, el conjunto de los automorfismos; todo automorfismo α , aplicación biyectiva de $\mathcal{E}$ sobre $\mathcal{E}$ admite una aplicación inversa α^{-1} , la cual es evidentemente lineal. Por otra parte, el producto de dos aplicaciones lineales α_1 y α_2 es también una aplicación lineal y si α_1 y α_2 son aplicaciones biyectivas de $\mathcal{E}$ sobre $\mathcal{E}$, el producto es una aplicación biyectiva de $\mathcal{E}$ sobre $\mathcal{E}$. Luego el producto de dos aplicaciones lineales regulares es también una aplicación lineal regular.

Su conjunto es efectivamente un grupo, llamado *grupo lineal* $\mathcal{L}_n$ para la dimensión n .

Una aplicación *singular* σ no puede tener inversa. En efecto, por hipótesis, existe un vector $x \neq 0$ tal que $\sigma x = 0$ de donde:

$$\forall \sigma' \in \mathcal{A} \quad (\sigma' \sigma)x = \sigma'(\sigma x) = \sigma'0 = 0,$$

por consiguiente

$$\sigma' \sigma \neq I.$$

Volvamos a las matrices y consideremos, en primer lugar, dos espacios cualesquiera

$$\mathcal{E} = (e_1, \dots, e_n) \quad \mathcal{E}' = (e'_1, \dots, e'_p);$$

a una aplicación regular α de $\mathcal{E}$ en $\mathcal{E}'$ corresponde la matriz- $(p \times n)$ A :

$$A = \| a_{ik} \| \quad \alpha(e_k) = \sum_i a_{ik} e'_i;$$

y nos proponemos caracterizar el rango r de la aplicación lineal α por medio de ciertas propiedades de la matriz A , representante de esta aplicación con las bases que han sido escogidas. Como dimensión del espacio imagen, r es igual al número máximo de vectores linealmente independiente entre los n vectores *columnas*

$$C_k = \alpha(e_k) \in \mathcal{E}', \quad (k = 1, \dots, n).$$

Pero podemos también asociar a las p filas de A los *vectores-filas* $L_1, \dots, L_p$ definidos por

$$L_i = \sum_{j=1}^n a_{ij} e_j \in \mathcal{E}, \quad (i = 1, \dots, p).$$

Estudiemos el número máximo l de vectores linealmente independientes entre estos p vectores-filas.

Teorema 1. — En una matriz rectangular A , el número máximo l de vectores filas linealmente independientes y el número máximo r de vectores columnas linealmente independientes son iguales:

$$r = l.$$

Puede esto enunciarse, también, diciendo que el rango de una matriz se conserva por transposición; entendiéndose por *transpuesta*, A' o A^T , de una matriz A , la que se obtiene al cambiar las filas por las columnas de A :

$$A' = \| a'_{ij} \|, \quad a'_{ij} = a_{ji}.$$

Por ejemplo, si $A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$, se tiene $A' = \begin{vmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \end{vmatrix}$

Demostración directa.

Establezcamos primeramente la desigualdad $r \leq l$.

Consideremos una relación de dependencia entre los vectores columnas:

$$(4) \quad \lambda_1 C_1 + \dots + \lambda_n C_n = 0, \quad \lambda_i \in \Delta.$$

Basta entonces aplicar esta desigualdad no solamente a la matriz dada, sino también a la matriz transpuesta, lo que, intercambiando r y l , conduce a la condición

$$l \leq r \quad \text{de donde} \quad l = r.$$

Demostración utilizando la noción de determinante ¹.

Dada una matriz- $p \times n$ $A = \| a_{ij} \|$, si tomamos un entero $q \leq p$ y n , podemos elegir en A , q filas y q columnas y considerar la matriz A_q formada por los elementos de estas q filas y q columnas; esta es una matriz cuadrada de orden q , y su determinante es lo que se llama un *menor* de orden q de A .

Vamos a designar por ρ el mayor valor de q tal, que exista algún menor de orden q que sea distinto de cero, y nos proponemos demostrar el teorema siguiente:

Teorema 2. — *El rango de la matriz A es igual al número ρ .*

Lema. — *Para que q vectores del espacio $\mathcal{E} = (e_1, \dots, e_n)$*

$$x_i = \sum_{j=1}^n a_{ij} e_j \quad (i = 1, 2, \dots, q)$$

sean linealmente independientes, es necesario y suficiente, que para la

$$\text{matriz- } q \times n \quad A'' = \| a_{ij} \| \quad (i = 1, \dots, q),$$

el orden ρ sea igual a q .

¹ En esta demostración y en la del párrafo 6, utilizaremos los determinantes. Las nociones de álgebra externa, en particular la de forma multilineal alternada, sobre las cuales se funda generalmente la introducción de los determinantes, no forman parte de nuestro programa, y nos limitaremos a recordar los principios siguientes:

A cada matriz cuadrada A de orden n de elementos de un cuerpo o más generalmente de un anillo conmutativo, se asocia, bajo el nombre de determinante, una cierta expresión polinómica de elementos, $|A|$ o $\det A$, tal, que $\det A = 0$ sea una condición necesaria y suficiente para que la ecuación $Ax = 0$ admita como solución al menos un vector x no nulo.

Para

$$A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix},$$

Supongamos primero los vectores $x_1, \dots, x_q$ dependientes y demostremos que se tiene $\rho \neq q$ (es decir $\rho < q$ ya que siempre es $\rho \leq q$). Supongamos por ejemplo que x_1 depende de los otros vectores:

$$x_1 = \lambda_2 x_2 + \dots + \lambda_q x_q,$$

lo que implica

$$a_{1j} = \sum_{k=2}^q \lambda_k a_{kj} \quad (j = 1, 2, \dots, n).$$

Entonces la matriz A'' toma la forma

$$A'' = \begin{vmatrix} \sum_{k=2}^q \lambda_k a_{k1} & \dots & \sum_{k=2}^q \lambda_k a_{kn} \\ a_{21} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{q1} & \dots & a_{qn} \end{vmatrix}$$

Los elementos de la primera fila son combinación lineal, con los mismos coeficientes, de los elementos de las filas siguientes. Resulta, suponiendo primeramente $q \leq n$, que todo determinante de orden q sacado de A'' (menor de orden q) tendrá esta propiedad y, por consiguiente, será nulo, de donde $\rho < q$. Si es $q > n$, como ρ es a lo sumo igual a n , la desigualdad $\rho < q$ se verifica también.

Recíprocamente, si $\rho < q$, $x_1, \dots, x_q$ son linealmente dependientes. Para demostrarlo, supongamos que tenemos un menor de orden ρ no nulo y que todo menor de orden $> \rho$ (si existe) sea nulo. Pueden hacerse siempre permutaciones

se tiene $\det A = a_{11} a_{22} - a_{12} a_{21}$ y se puede definir, por recurrencia sobre n , el determinante de una matriz $A = ||a_{ij}||$ de orden n por la fórmula

$$A = \sum_{i=1}^n A_{ji} a_{ij}$$

donde A_{ji} designa el producto por $(-1)^{i+j}$ del determinante de la matriz deducida de A por supresión de la fila i y de la columna j ("menor con su signo").

Utilizaremos también las relaciones fundamentales

$$0 = \sum_{i=1}^n A_{ji} a_{ik} \quad \text{para } j \neq k.$$

Además, para el producto de dos matrices cuadradas de orden n , A y B se tiene:

$$\det (AB) = \det A \cdot \det B.$$

de filas y de columnas tales que el menor distinto de cero en cuestión se escriba:

$$D = \begin{vmatrix} a_{11} & \dots & a_{1\rho} \\ \dots & \dots & \dots \\ a_{\rho 1} & \dots & a_{\rho\rho} \end{vmatrix}$$

por lo demás, tales permutaciones de filas y de columnas tienen solamente por efecto cambiar el orden de los correspondientes vectores, lo que no influye sobre las propiedades de independencia lineal. Por consiguiente, es lícito suponer que el menor no nulo es D . Formemos, a partir de la matriz de la cual D es el determinante, la matriz siguiente:

$$C = \left\| \begin{array}{cccc} a_{1,1} & \dots & a_{\rho 1} & c_1 \\ \dots & \dots & \dots & \dots \\ a_{\rho 1} & \dots & a_{\rho\rho} & c_\rho \\ a_{\rho+1,1} & \dots & a_{\rho+1,\rho} & c_{\rho+1} \end{array} \right\|$$

llamemos D_i el menor de c_i en C (con su signo): $D_{\rho+1} = D \neq 0$; remplazando c_1 por a_{1j} , ..., $c_{\rho+1}$ por $a_{\rho+1,j}$ obtendremos el determinante

$$\begin{vmatrix} a_{1,1} & \dots & a_{1,\rho} & a_{1j} \\ \dots & \dots & \dots & \dots \\ a_{\rho+1,1} & \dots & a_{\rho+1,\rho} & a_{\rho+1,j} \end{vmatrix}$$

que es nulo, pues si $j = 1, 2, \dots, \rho$, tiene dos columnas idénticas, y si

$$j = \rho + 1, \dots, n,$$

es un menor de orden $\rho + 1$ sacado de la matriz A' . Si lo desarrollamos según los elementos de la última columna, nos da:

$$D_1 a_{1,j} + \dots + D_\rho a_{\rho,j} + D a_{\rho+1,j} = 0 \quad (j = 1, 2, \dots, n)$$

es decir

$$D_1 x_1 + \dots + D_\rho x_\rho + D x_{\rho+1} = 0, \quad \text{con} \quad D \neq 0,$$

dicho de otro modo, $x_1, x_2, \dots, x_q$ son linealmente dependientes.

Siendo esto así, según el recíproco del lema, $\rho + 1$ vectores filas de la matriz A son siempre linealmente dependientes, y según la primera parte, existe un sistema de ρ vectores filas linealmente independientes, pues de otro modo todo

menor de orden ρ sacado de A sería nulo. Tenemos por consiguiente:

$$l = \rho.$$

Pero ρ es evidentemente el mismo para la matriz A y para su transpuesta, y si se aplica el mismo razonamiento a la matriz transpuesta, se obtiene

$$r = l$$

siendo r el número de vectores columnas linealmente independientes. Por consiguiente

$$l = \rho = r.$$

Se encuentra así, de nuevo, la igualdad del número máximo l de vectores filas linealmente independientes y del número máximo r de vectores columnas linealmente independientes; por otra parte su valor común resulta ser el orden máximo de los menores no nulos de la matriz.

Caso particular. Matrices cuadradas. — *Para que una matriz cuadrada A de orden n sea regular, es necesario y suficiente que los vectores columnas sean independientes, es decir $r = n$, lo que quiere decir, también, que $\rho = n$. Ahora bien, no hay aquí más que un menor de orden n , que es el determinante de A .*

Por tanto, para que A sea regular, es necesario y suficiente que su determinante sea distinto de cero y, por consiguiente, las matrices singulares son aquellas cuyo determinante es nulo.

Veamos una demostración directa de este resultado importante. Se trata de estudiar, desde el punto de vista de la independencia lineal los vectores

$$ae_k = \sum_{i=1}^n a_{ik} e_i;$$

supongamos que existe entre ellos una relación:

$$\sum_{k=1}^n \lambda_k ae_k = \sum_{k,i} \lambda_k a_{ik} e_i = 0,$$

Puesto que los e_i son linealmente independientes, esto equivale al sistema siguiente de n ecuaciones lineales y homogéneas con n incógnitas $\lambda_1, \dots, \lambda_n$:

$$\sum_k \lambda_k a_{ik} = 0 \quad (i = 1, 2, \dots, n)$$

Para que los vectores αe_k sean linealmente independientes es necesario y suficiente que la única solución de este sistema sea la solución trivial

$$\lambda_1 = \dots = \lambda_n = 0,$$

es decir que el determinante D de A no sea nulo.

Se ve fácilmente que la matriz inversa A^{-1} de la matriz regular A se escribe

$$A^{-1} = \frac{1}{D} \begin{vmatrix} A_{11} & \dots & A_{1n} \\ \dots & \dots & \dots \\ A_{n1} & \dots & A_{nn} \end{vmatrix}$$

donde $A_{\lambda\mu}$ designa el menor de $a_{\mu\lambda}$ (tomado con su signo).

§ 4. Cambio de base

En un espacio vectorial $\mathcal{E}$ de dimensión n sobre el cuerpo Δ , consideremos dos bases:

$$\mathcal{E} = (e_1, e_2, \dots, e_n) = (\nu_1, \nu_2, \dots, \nu_n).$$

Expresemos cada vector de una base como combinación lineal de los vectores de la otra:

$$(1) \quad e_\lambda = \sum_i t_{i\lambda} \nu_i, \quad (2) \quad \nu_k = \sum_\mu t'_{\mu k} e_\mu$$

de donde

$$\begin{aligned} e_\lambda &= \sum_i t_{i\lambda} \left(\sum_\mu t'_{\mu i} e_\mu \right) \\ &= \sum_\mu \left(\sum_i t'_{\mu i} t_{i\lambda} \right) e_\mu \quad (\lambda = 1, 2, \dots, n) \end{aligned}$$

pero los e_λ son vectores linealmente independientes, por consiguiente, las relaciones precedentes exigen:

$$\sum_i t'_{\mu i} t_{i\lambda} = \delta_{\lambda\mu}$$

Si consideramos las matrices cuadradas de orden n

$$T = \| t_{i\lambda} \| \quad \text{y} \quad T' = \| t'_{\mu i} \|$$

se ve que

$$T'T = I.$$

Las dos *matrices* de nuestro *cambio de coordenadas* son inversas una de otra y por consiguiente *regulares*.

Escribiremos, fundados en lo que precede, T^{-1} en vez de T' .

Dada la matriz A que representa una aplicación α en la primera base, propongámonos determinar la matriz B que representa α en la segunda base $(v_1, \dots, v_n)$.

Tenemos, en la base antigua

$$\alpha e_k = \sum_i a_{ik} e_i$$

y en la base nueva

$$\alpha v_k = \sum_j b_{jk} v_j.$$

Se puede escribir

$$\begin{aligned} \alpha v_k &= \alpha \left(\sum_{\mu} t'_{\mu k} e_{\mu} \right) = \sum_{\mu} t'_{\mu k} (\alpha e_{\mu}) \\ &= \sum_{\mu} \sum_i t'_{\mu k} a_{i\mu} e_i = \sum_{\mu} \sum_i \sum_j t'_{\mu k} a_{i\mu} t_{ji} v_j \\ &= \sum_{i,j,\mu} t_{ji} a_{i\mu} t'_{\mu k} v_j \end{aligned}$$

de donde

$$b_{jk} = \sum_{i,\mu} t_{ji} a_{i\mu} t'_{\mu k},$$

lo que da:

$$B = TAT' = TAT^{-1},$$

y concluimos: B es la matriz transformada de A por la matriz T del cambio de base.

Las matrices A y TAT^{-1} se llaman *equivalentes*.

Propiedades de la transformación de matrices.

La transformación de matrices por una matriz T (que debe ser evidentemente

siempre regular) tiene las propiedades siguientes:

$$\begin{aligned}T(A_1 + A_2)T^{-1} &= TA_1T^{-1} + TA_2T^{-1} \\T(\lambda A)T^{-1} &= \lambda TAT^{-1} \quad (\lambda \in \Delta) \\(TAT^{-1})^m &= TAT^{-1} \cdot TAT^{-1} \dots = TA^mT^{-1}.\end{aligned}$$

Si nos dan un polinomio $f(u) \in \Delta[u]$, anillo de los polinomios en u con coeficientes de Δ , podemos reemplazar la indeterminada u por una matriz A y considerar la matriz:

$$f(A) = a_0A^m + a_1A^{m-1} + \dots + a_mI.$$

Combinando las reglas precedentes, vemos que se tiene:

$$f(TAT^{-1}) = Tf(A)T^{-1}$$

Puede acontecer que, para determinados polinomios f del anillo $\Delta[u]$, $f(A)$ sea la *matriz cero*. Se dice entonces que A verifica la *ecuación matricial*

$$f(u) = 0.$$

Resulta inmediatamente que si una matriz A anula a un polinomio f , todas sus transformadas TAT^{-1} anulan también a f . Este hecho era evidente *a priori* ya que, si α designa la aplicación lineal de la que A es la matriz con la base $(e_1, \dots, e_n)$, la ecuación $f(A) = 0$ significa que la aplicación lineal

$$f(\alpha) = a_0\alpha^m + a_1\alpha^{m-1} + \dots + a_mI$$

es la aplicación cero, $f(\alpha) = \theta$. Esta propiedad, por ser independiente de la base escogida, implica $f(TAT^{-1}) = 0$ para toda matriz regular T .

Observación. — La matriz

$$f(A) = a_0A^m + a_1A^{m-1} + \dots + a_mI$$

se escribe también

$$f(A) = (a_0I)A^m + (a_1I)A^{m-1} + \dots + a_mI;$$

puede, pues, mirarse como el resultado de la sustitución de la matriz A en el polinomio

$$F(u) = (a_0I)u^m + (a_1I)u^{m-1} + \dots + a_mI \in \mathcal{M}[u],$$

el anillo de polinomios $\mathcal{M}[u]$ es por lo demás una extensión del anillo $\Delta[u]$, puesto que el cuerpo Δ es isomorfo al subconjunto de $\mathcal{M}$ constituido por las matrices escalares, que no es otro que el centro de $\mathcal{M}$.

La ecuación $F(u) = 0$ tiene, en el anillo $\mathcal{M}$, con la solución A , el conjunto de soluciones TAT^{-1} , lo que pone en evidencia la diferencia entre las propiedades de las ecuaciones algebraicas en el caso clásico y en el caso que ahora tratamos de un anillo no conmutativo con divisores de cero.

Vamos a ver que existen siempre polinomios $f \in \Delta[u]$ tales, que la matriz $f(A)$ sea la matriz cero.

§ 5. Ecuación mínima

En el conjunto $\mathcal{M}$ de las matrices $(n \times n)$ sobre el cuerpo Δ , consideremos una matriz A y la sucesión de matrices

$$I = A^0, A^1, \dots, A^k, \dots$$

Por ser $\mathcal{M}$ un espacio vectorial de dimensión n^2 , no puede haber más de n^2 matrices linealmente independientes. Algunas matrices de la sucesión precedente dependerán, pues, linealmente de las precedentes; sea μ el menor valor de k para que eso ocurra ($\mu \leq n^2$):

$$\lambda_0 A^\mu + \lambda_1 A^{\mu-1} + \dots + \lambda_\mu I = 0, \quad \lambda_0 \neq 0, \quad \lambda_i \in \Delta.$$

La matriz A anula al polinomio

$$\lambda_0 u^\mu + \dots + \lambda_\mu.$$

En el anillo principal $\Delta[u]$, el conjunto $\mathfrak{m}$ de los polinomios anulados por la matriz A es un *ideal*, pues las potencias de A son permutables entre ellas y con los elementos de Δ y, por lo tanto, el principio de substitución se aplica cuando se reemplaza u por A , y el producto de un polinomio de $\mathfrak{m}$ por un polinomio arbitrario es un polinomio de $\mathfrak{m}$. El ideal $\mathfrak{m}$ es *principal*:

$$\mathfrak{m} = (m).$$

El polinomio generador $m(u)$ está definido salvo un factor de Δ ; esto puede aprovecharse para hacer que el coeficiente de su término de mayor grado sea el elemento unidad de Δ . Con esto $m(u)$ está perfectamente definido; se le llama *polinomio mínimo* de la matriz A , y se llama *ecuación mínima* de A la ecuación $m(u) = 0$.

A toda matriz quedan asociados un polinomio mínimo y una ecuación mínima. Desde luego, lo que precede se aplica también a la aplicación lineal α que la matriz representa cuando se escoge en el espacio vectorial $\mathfrak{E}$ una base, y se dirá también que $m(u) = 0$ es la ecuación mínima de esta aplicación lineal α .

Estudiemos esta ecuación mínima; mostremos particularmente que juega un papel fundamental en el estudio de los *subespacios invariantes* en la aplicación α es decir, en los subespacios $\mathfrak{S} \subseteq \mathfrak{E}$ tales que

$$\alpha\mathfrak{S} \subseteq \mathfrak{S}$$

($x \in \mathfrak{S}$ implica $\alpha x \in \mathfrak{S}$).

Cuando se verifique esto, puede considerarse la *restricción* α' de α a $\mathfrak{S}$.

Para todo vector x de $\mathfrak{S}$, la relación

$$\alpha'x = \alpha x \quad (x \in \mathfrak{S})$$

implica

$$\alpha'^2x = \alpha^2x \quad (x \in \mathfrak{S})$$

y, sucesivamente,

$$\alpha'^kx = \alpha^kx, \quad (\forall k \in \mathbb{N}).$$

Por tanto la restricción de una potencia de α es la potencia de la restricción de α , de suerte que, siendo $f(u)$ un polinomio de coeficientes en Δ , $f(\alpha)$ tendrá como restricción $f(\alpha')$:

$$f(\alpha')x = f(\alpha)x, \quad \forall x \in \mathfrak{S}$$

Resulta que $\mathfrak{S}$, *subespacio invariante de la aplicación α* , es también *subespacio invariante de $f(\alpha)$* , siendo $f(u)$ un polinomio cualquiera de coeficientes en Δ .

Si nos dan un polinomio $f(u)$ y si consideramos la aplicación lineal $f(\alpha)$, esta tiene un cierto *núcleo* $\mathcal{N}_{f(\alpha)}$:

$$\mathcal{N}_{f(\alpha)} = \{ x ; f(\alpha)x = 0 \}$$

que es un cierto subespacio de $\mathfrak{E}$. Se dice que este es el *espacio cero* (o *nulo*) del polinomio f .

Teorema 1. — *Cualquiera que sea el polinomio $f \in \Delta[u]$, $\mathcal{N}_{f(\alpha)}$ es un subespacio invariante para la aplicación α .*

Debemos demostrar que: $x \in \mathcal{N}_{f(\alpha)}$ implica $\alpha x \in \mathcal{N}_{f(\alpha)}$.

Para ello formemos:

$$f(a)(ax) = [f(a)a]x = [af(a)]x = a[f(a)x] = a0 = 0$$

y tenemos efectivamente que

$$ax \in \mathcal{N}_{f(a)}.$$

Propiedades de los núcleos. — Para simplificar las notaciones, escribiremos desde ahora $\mathcal{N}_f$ en vez de $\mathcal{N}_{f(a)}$.

1. Si $g(u)$ divide $f(u)$, $\mathcal{N}_g$ está contenido en $\mathcal{N}_f$, $\mathcal{N}_g \subseteq \mathcal{N}_f$.

En efecto, pongamos $f(u) = g(u)q(u)$ y apliquemos $f(a)$ a un vector x cualquiera

$$f(a)x = [g(a)q(a)]x = [q(a)g(a)]x = q(a)[g(a)x].$$

Si $x \in \mathcal{N}_g$, $g(a)x = 0$, de donde $f(a)x = q(a)0 = 0$, lo que implica $x \in \mathcal{N}_f$.

2. Consideremos ahora dos polinomios cualesquiera $f(u)$ y $g(u)$, y sea $d(u)$ su m.c.d.; el núcleo $\mathcal{N}_d$ de $d(a)$ es la intersección de los núcleos $\mathcal{N}_f$ y $\mathcal{N}_g$ de $f(a)$ y $g(a)$:

$$\mathcal{N}_d = \mathcal{N}_f \cap \mathcal{N}_g.$$

Según lo que precede, tendremos $\mathcal{N}_d \subseteq \mathcal{N}_f$ y $\mathcal{N}_d \subseteq \mathcal{N}_g$, luego

$$\mathcal{N}_d \subseteq \mathcal{N}_f \cap \mathcal{N}_g.$$

Establezcamos la inclusión inversa; tenemos, en el anillo euclídeo $\Delta[u]$, la relación de Bezout

$$d(u) = r(u)f(u) + s(u)g(u).$$

Reemplacemos u por a y apliquemos los dos miembros a $x \in \mathfrak{E}$:

$$\begin{aligned} d(a)x &= [r(a)f(a) + s(a)g(a)]x. \\ &= r(a)f(a)x + s(a)g(a)x. \end{aligned}$$

Si $x \in \mathcal{N}_f \cap \mathcal{N}_g$,

$$f(a)x = g(a)x = 0, \quad \text{luego} \quad d(a)x = 0,$$

lo que implica que $x \in \mathcal{N}_d$.

Primer caso particular: $f(u)$ y $g(u)$ son primos entre sí.

El m.c.d. (f, g) es una constante, que puede ser reducida al elemento unidad e :

$$\mathcal{N}_e = \{x; Ix = 0\} = \{0\},$$

la intersección de $\mathcal{N}_f$ y $\mathcal{N}_g$ es el vector cero.

Segundo caso particular: $g(u) = m(u)$ es el polinomio mínimo de α , siendo $f(u)$ cualquiera.

Entonces, por ser $m(\alpha)$ la aplicación nula:

$$\mathcal{N}_{m(\alpha)} = \mathcal{N}_\theta = \{x; \theta x = 0\} = \mathcal{E}$$

el núcleo de m es el espacio entero, y tenemos, en este caso,

$$\mathcal{N}_f \cap \mathcal{N}_m = \mathcal{N}_f \cap \mathcal{E} = \mathcal{N}_f = \mathcal{N}_{\text{m.c.d.}(f, m)}$$

El núcleo de $f(\alpha)$ no cambia cuando se reemplaza f por su m.c.d. con el polinomio mínimo m . El m.c.d. de un polinomio cualquiera con m debe ser un divisor de m , por lo que obtendremos todos los casos posibles para $\mathcal{N}$ examinando lo que ocurre para los diferentes divisores del polinomio mínimo m .

3. Caso de divisores sucesivos de $m(u)$: si $f(u)$ divide a $m(u)$, y si $g(u)$ divide a $f(u)$ siendo g un divisor propio de f (grado de $g <$ grado de f), se tiene la inclusión estricta $\mathcal{N}_g \subset \mathcal{N}_f$; luego también $\dim \mathcal{N}_g < \dim \mathcal{N}_f$.

Puesto que g divide a f , se sabe que $\mathcal{N}_g \subseteq \mathcal{N}_f$, basta por tanto demostrar que $\mathcal{N}_g$ es distinto de $\mathcal{N}_f$. Pongamos:

$$\begin{aligned} m(u) &= f(u)h(u), \\ f(u) &= g(u)\gamma(u) \text{ grado de } \gamma > 0, \end{aligned}$$

de donde

$$m(u) = g(u)h(u)\gamma(u) = k(u)\gamma(u),$$

con

$$k(u) = g(u)h(u),$$

y como el grado de γ es positivo, $k(u)$ es un divisor propio de $m(u)$. Si se reemplaza la indeterminada u por la aplicación lineal dada α , se ve que:

$$k(\alpha) = g(\alpha)h(\alpha) \neq \theta$$

ya que, en caso contrario, $m(\alpha)$ no sería el polinomio mínimo. En consecuencia, existe un vector x tal que

$$k(\alpha)x = g(\alpha)h(\alpha)x \neq 0.$$

Entonces, el vector $y = h(\alpha)x$ no pertenece al núcleo $\mathcal{N}_g : y \notin \mathcal{N}_g$. En tanto se tiene

$$f(\alpha)y = f(\alpha)h(\alpha)x = m(\alpha)x = \theta x = 0$$

luego $y \in \mathcal{N}_f$; tenemos efectivamente la inclusión estricta: $\mathcal{N}_g \subset \mathcal{N}_f$.

Aplicación. — Sabemos ya que si f es primo con el polinomio mínimo m , su núcleo se reduce al subespacio nulo. Vamos a probar que *este es el único caso en que $\mathcal{N}_f$ se reduce al espacio nulo*. Dicho de otro modo, si el m.c.d. de f y m es un polinomio propio de grado positivo, entonces, el núcleo de $\mathcal{N}_f$ es un subespacio de dimensión positiva. En efecto, la propiedad 3 que antecede se aplica con $g = e$; g divide estrictamente al m.c.d. de f y m , luego

$$\mathcal{N}_e = \{0\} \subset \mathcal{N}_d = \mathcal{N}_f.$$

Así, para que el núcleo de la aplicación $f(\alpha)$ sea de dimensión positiva, es necesario y suficiente que el m.c.d. de f y m sea de grado positivo.

4. Consideremos un divisor $f(u)$ del polinomio mínimo $m(u)$ de la aplicación lineal α . Supongamos que $f(u)$ sea de grado positivo y que el coeficiente de su término de más alto grado se haya reducido a la unidad, $e \in \Delta$. Sabemos (teorema 1) que el núcleo $\mathcal{N}_{f(\alpha)}$ es un subespacio invariante para α y se puede hablar de la restricción α' de α al subespacio $\mathcal{N}_f$; veamos que el polinomio $f(u)$ es el polinomio mínimo de α' .

Llamemos $\mu(u)$ al polinomio mínimo de α' . La restricción de $f(\alpha)$ a $\mathcal{N}_f$ es $f(\alpha')$:

$$f(\alpha')x = f(\alpha)x \quad \text{si} \quad x \in \mathcal{N}_f;$$

luego, según la propia definición de $\mathcal{N}_f$:

$$f(\alpha')x = 0, \quad \forall x \in \mathcal{N}_f,$$

$f(\alpha')$ es la aplicación nula, θ' , de $\mathcal{N}_f$ en sí mismo. Luego $f(u)$ es un múltiplo de $\mu(u)$ y por consiguiente $\mathcal{N}_\mu \subseteq \mathcal{N}_f$.

Recíprocamente, consideremos el vector transformado de $x \in \mathcal{N}_f$ por $\mu(a)$:

$$\mu(a)x = \mu(a')x = \theta'x = 0, \quad \forall x \in \mathcal{N}_f.$$

luego $\mu(a)$ transforma cualquier vector $x \in \mathcal{N}_f$ en el vector cero, y por lo tanto

$$\mathcal{N}_f \subseteq \mathcal{N}_\mu, \quad \text{donde} \quad \mathcal{N}_f = \mathcal{N}_\mu.$$

siendo $\mu(u)$ divisor de $f(u)$, es imposible, según la propiedad 3, que sea un divisor propio, de donde

$$f(u) = \mu(u).$$

5. Consideremos ahora r polinomios, $f_1(u), \dots, f_r(u)$, los núcleos $\mathcal{N}_1, \dots, \mathcal{N}_r$ de las aplicaciones correspondientes, y su m.c.m. $h(u)$. Vamos a mostrar que

$$\mathcal{N}_h = \mathcal{N}_1 + \dots + \mathcal{N}_r$$

Pongamos

$$(1) \quad h(u) = f_i(u)h_i(u) \quad (i = 1, 2, \dots, r)$$

siendo los h_i primos entre sí en su conjunto, lo que se traduce por la relación de Bezout generalizada

$$(2) \quad s_1(u)h_1(u) + \dots + s_r(u)h_r(u) = e, \quad s_i(u) \in \mathcal{A}[u]$$

(que se establece fácilmente por recurrencia sobre r).

Como f_i divide a h , se tiene

$$\mathcal{N}_i \subseteq \mathcal{N}_h$$

y por consiguiente:

$$\mathcal{N}_1 + \dots + \mathcal{N}_r \subseteq \mathcal{N}_h.$$

Veamos que se cumple la inclusión inversa. Según la identidad (2) se puede escribir, para todo vector x de $\mathcal{E}$,

$$\text{es decir} \quad x = Ix = [s_1(a)h_1(a) + \dots + s_r(a)h_r(a)]x$$

$$(3) \quad x = s_1(a)h_1(a)x + \dots + s_r(a)h_r(a)x ;$$

para un vector $x \in \mathcal{N}_h$, tenemos:

$$h(\alpha)x = 0,$$

es decir, según la relación (1):

$$f_i(\alpha)h_i(\alpha)x = 0,$$

lo que demuestra que

$$h_i(\alpha)x \in \mathcal{N}_i.$$

Pero se sabe que $\mathcal{N}_i$ es un subespacio invariante de α , de todas sus potencias y de todo polinomio en α , en particular de $s_i(\alpha)$. Por consiguiente el vector $x_i = s_i(\alpha)h_i(\alpha)x$ pertenece a $\mathcal{N}_i$ (en cuanto $x \in \mathcal{N}_h$), y (3) se escribe:

$$(4) \quad x = x_1 + \dots + x_i + \dots + x_r \quad \forall x \in \mathcal{N}_h$$

con $x_i \in \mathcal{N}_i$; luego

$$\mathcal{N}_h \subseteq \mathcal{N}_1 + \dots + \mathcal{N}_r,$$

y, en consecuencia, vale la igualdad.

Supongamos ahora los polinomios f_i primos entre si dos a dos; su m.c.m. h es entonces su producto.

Uno cualquiera de estos polinomios f_i , es primo con $f_1, \dots, f_{i-1}, f_{i+1}, \dots, f_r$, luego lo es con su producto y tendremos, según la propiedad 2,

$$\mathcal{N}_i \cap (\mathcal{N}_1 + \dots + \mathcal{N}_{i-1} + \mathcal{N}_{i+1} + \dots + \mathcal{N}_r) = 0 \quad (i = 1, \dots, r)$$

de donde resulta que la suma de los núcleos es directa. Podemos enunciar:

Cuando los polinomios f_i son primos entre si, el núcleo $\mathcal{N}_h$ de su producto h es la suma directa de sus núcleos:

$$\mathcal{N}_h = \mathcal{N}_1 \oplus \dots \oplus \mathcal{N}_r$$

y por consiguiente cada vector $x \in \mathcal{N}_h$ es, de un modo único, la suma de vectores $x_i \in \mathcal{N}_i$:

$$x = x_1 + \dots + x_r.$$

Aplicación al polinomio mínimo $m(u)$ de α . — Consideremos la descomposición de $m(u)$ en factores irreducibles sobre el cuerpo Δ :

$$m(u) = [q_1(u)]^{\rho_1} \dots [q_r(u)]^{\rho_r} \quad (\rho_i \geq 1, r \geq 1)$$

teniendo los factores $q_i(u)$ coeficientes de Δ . Por ser irreducibles, estos factores son necesariamente primos entre sí dos a dos, y lo mismo sus potencias. Se puede aplicar lo precedente; como $m(\alpha) = \theta$, el núcleo $\mathcal{N}_{m(\alpha)}$ es el espacio $\mathfrak{E}$ y vemos que:

$$\mathcal{N}_{m(\alpha)} = \mathfrak{E} = \mathcal{N}_1 \oplus \dots \oplus \mathcal{N}_r$$

llamando $\mathcal{N}_i$ al núcleo de

$$[q_i(\alpha)]^{\rho_i}$$

podemos enunciar, pues, el fundamental resultado siguiente:

Teorema 2. — *A la descomposición en factores irreducibles del polinomio mínimo $m(u)$ sobre el cuerpo Δ corresponde una descomposición del espacio $\mathfrak{E}$ en suma directa de subespacios cuyo número es igual al número de factores distintos que figuran en la descomposición de $m(u)$.*

Designemos por ν_i la *dimensión* del subespacio $\mathcal{N}_i$ y en cada uno de estos subespacios tomemos una base:

$$\mathcal{N}_i = (\nu_{i1}, \dots, \nu_{i\nu_i}).$$

Uniendo estas bases obtenemos una base de $\mathfrak{E}$.

$$(5) \quad (\nu_{11}, \dots, \nu_{r\nu_r}) = \mathfrak{E}$$

pues

$$\mathcal{N}_i = (\nu_{i1}) \oplus \dots \oplus (\nu_{i\nu_i}).$$

Resulta que, si n es la dimensión de $\mathfrak{E}$, tenemos

$$n = \nu_1 + \dots + \nu_r.$$

Volviendo a la aplicación lineal α , examinemos el aspecto de la matriz A que la representa cuando se toma para $\mathfrak{E}$ la base (5) (base, por lo demás, no definida de modo único, en general). Para ello, examinemos cómo se transforma por α el vector de base $\nu_{ij} \in \mathcal{N}_i$. Puesto que $\mathcal{N}_i$ es un subespacio invariante para α , $\alpha\nu_{ij} \in \mathcal{N}_i$; resulta que la componente de $\alpha\nu_{ij}$ respecto a uno cualquiera de los vectores de base situados fuera de $\mathcal{N}_i$ es nula. Nos vemos conducidos a

distinguir en la matriz

$$A = \begin{array}{c|ccc|c} & \overbrace{\quad}^{v_1} & & \overbrace{\quad}^{v_i} & & \overbrace{\quad}^{v_r} & \\ \hline & & & 0 & & & \} v_1 \\ \hline & & & 0 & & & \\ \hline & & & & & & \\ \hline & & & & & & \} v_i \\ \hline & & & 0 & & & \\ \hline & & & 0 & & & \} v_r \\ \hline & & & & & & \end{array}$$

agrupaciones de $v_1, \dots, v_i, \dots$ líneas y columnas. La columna donde figuran las coordenadas de $\alpha v_{ij} \in \mathcal{N}_i$ está situada en el grupo de orden i ; los elementos de esta columna son nulos, salvo los que corresponden a los vectores de base de $\mathcal{N}_i$, los que están situados sobre las v_i filas de la agrupación de orden i .

Aparte de los cuadrados que tienen como diagonal la diagonal principal de A , y que corresponden a los subespacios $\mathcal{N}_i$, todos los elementos son ceros, y la matriz tiene el aspecto siguiente:

$$A = \begin{array}{c|ccc|c} & \boxed{A_1} & & & & \\ \hline & & \boxed{A_2} & & & \\ \hline & & & \ddots & & \\ \hline & & & & \boxed{A_i} & \\ \hline & & & & & \leftarrow \mathcal{N}_i \\ \hline & & & & & \\ \hline & & & & & \boxed{A_r} \\ \hline \end{array}$$

esta matriz aparece descompuesta en r submatrices a lo largo de la diagonal principal, y fuera de ellas no tiene más que ceros. Designemos por A_i la matriz que corresponde a $\mathcal{N}_i$: es la matriz de la restricción α'_i de α al subespacio invariante $\mathcal{N}_i$. Pero, según la propiedad 4, sabemos que el polinomio mínimo de α'_i

o de la matriz correspondiente A_i , no es otra cosa que el divisor correspondiente de $m(u)$, es decir,

$$[q_i(u)]^{p_i}$$

Así hemos encontrado una *forma reducida notable* de A que corresponde a una descomposición del espacio en suma directa.

§ 6. Ecuación característica

Un caso notable es aquel en que el cuerpo considerado Δ es el de los números complejos, como vamos a suponer desde ahora. En este caso el polinomio $m(u)$ se descompone en *factores lineales*.

De modo general, busquemos primero con qué condición un polinomio de primer grado

$$f(u) = u - \lambda, \quad \lambda \in \Delta,$$

divide al polinomio mínimo $m(u)$ de la aplicación lineal α .

Teorema 1. — *Para que $f(u) = u - \lambda$ ($\lambda \in \Delta$) divida al polinomio $m(u)$ de α , es necesario y suficiente que exista en el espacio vectorial $\mathfrak{E}$ considerado, un vector no nulo x satisfaciendo a la ecuación*

$$(1) \quad (\alpha - \lambda I)x = 0.$$

1.º Si m es de grado 1, y si $f = u - \lambda$ divide a m , tenemos $m = f$, luego $m(\alpha) = \alpha - \lambda I = \theta$; α es una homotecia, la matriz correspondiente A es una matriz escalar, y todo vector no nulo x se transforma en 0 por $\alpha - \lambda I = \theta$.

Si m es de grado > 1 , $f = u - \lambda$ es un divisor propio, el núcleo $\mathcal{N}_f$ tiene dimensión > 0 : existe en efecto un vector no nulo $x \in \mathcal{N}_f$, tal que $f(\alpha)x = 0$, es decir

$$(\alpha - \lambda I)x = 0.$$

2.º Recíprocamente, supongamos que exista un vector $x \neq 0$ tal que

$$(\alpha - \lambda I)x = 0.$$

es decir, que x pertenece al núcleo $\mathcal{N}_{f(\alpha)}$ poniendo $f(u) = u - \lambda$. Pero

$$\mathcal{N}_{f(\alpha)} = \mathcal{N}_{\text{m. c. d. } (f, m)}$$

y puesto que este núcleo es de dimensión ≥ 1 , el m.c.d. tiene de grado al menos 1, lo que exige, por ser f de grado 1, que este m.c.d. sea el propio f . Luego f divide a $m(u)$.

Es fácil expresar de otro modo la condición precedente. Tomemos una base de $\mathfrak{E}$ y llamemos $A = \| a_{ij} \|$ la matriz de α en esa base; la aplicación lineal $\alpha - \lambda I$ tiene por matriz

$$\| a_{ij} - \lambda \delta_{ij} \|$$

y la relación (1) es equivalente al sistema de ecuaciones (1') que se obtiene al escribir que cada coordenada del vector $(\alpha - \lambda I)x$ es nula, o sea, designando por ξ_k las coordenadas de x :

$$(1') \quad \sum_{k=1}^n (a_{ik} - \lambda \delta_{ik}) \xi_k = 0, \quad (i = 1, \dots, n).$$

La condición del teorema 1 significa que existe un sistema de n coordenadas $\xi_1, \dots, \xi_n$ no todas nulas, satisfaciendo al sistema (1'). Para ello es necesario y suficiente que el determinante del sistema sea nulo

$$\begin{vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \lambda \end{vmatrix} = 0$$

lo que se escribe

$$| A - \lambda I | = 0 \quad \text{donde} \quad \det(A - \lambda I) = 0.$$

Esta es una ecuación en λ cuyo primer miembro se indica por $(-1)^n \varphi(\lambda)$. Se llama a $\varphi(\lambda)$ el *polinomio característico de la aplicación α* , y $\varphi(\lambda) = 0$ es su *ecuación característica*.

Vemos con esto que todo cero λ del polinomio mínimo es un cero del polinomio característico (de grado n) y que inversamente todo cero del polinomio característico es un cero del polinomio mínimo. Los dos polinomios $m(u)$ y $\varphi(u)$ tienen los mismos ceros (con órdenes de multiplicidad generalmente diferentes); estos ceros se llaman los *valores característicos* (también *valores propios*) de la matriz A o de la aplicación lineal α .

La ecuación característica expresa que la matriz $\| \alpha - \lambda I \|$ es *singular*; el conjunto de sus valores característicos se llama el *espectro* de la matriz A , o de la aplicación lineal α .

Para un valor característico λ , existe al menos un vector no nulo x que verifica la ecuación (1): un vector tal se llama *vector propio* de la aplicación lineal α , o de la matriz A . Geométricamente un vector propio es un vector tal que el subespacio que engendra (de dimensión 1, por lo que se llama *recta*) sea invariante de α .

Los vectores propios, los valores característicos y el polinomio característico de una aplicación lineal α son, por definición, entes independientes de la base elegida en el espacio $\mathfrak{E}$. Consideremos dos bases de este espacio

$$\mathfrak{E} = (a_1, \dots, a_n) = (b_1, \dots, b_n)$$

y las matrices equivalentes A y $B = TAT^{-1}$ que representan a α en una u otra de estas bases; T representa la matriz regular que ha definido el cambio de base (§ 4). Las matrices A y B tienen el mismo polinomio característico. Por lo demás, ello se comprueba fácilmente poniendo

$$B - \lambda I = TAT^{-1} - \lambda I = T(A - \lambda I)T^{-1}$$

de donde

$$\det(B - \lambda I) = \det(A - \lambda I)$$

puesto que los determinantes de T y de T^{-1} son inversos uno de otro.

Si desarrollamos el polinomio característico de la matriz $A = \|a_{ij}\|$

$$\varphi(\lambda) = \det(\lambda I - A) = \lambda^n - t_1\lambda^{n-1} + \dots + (-1)^n t_n$$

los coeficientes t_i de este polinomio son invariantes en todo cambio de base; el primero

$$t_1 = a_{11} + \dots + a_{nn},$$

suma de los elementos de la diagonal principal de la matriz A se llama la *traza* de la matriz A o de la aplicación lineal α que ella representa. La constante t_n es el determinante de A .

Consideremos una aplicación lineal α de $\mathfrak{E}$ en sí mismo y la matriz A que representa a α en una cierta base. Sea λ un valor característico; existe un vector $x \neq 0$ tal que

$$\alpha x = \lambda x.$$

Volvamos a aplicar α :

$$\alpha^2 x = \alpha(\lambda x) = \lambda(\alpha x) = \lambda^2 x.$$

De paso en paso obtenemos las igualdades siguientes:

$$(2) \quad \left\{ \begin{array}{l} (Ix = x) \\ ax = \lambda x \\ a^2x = \lambda^2x \\ \dots\dots\dots \\ a^kx = \lambda^kx \\ \dots\dots\dots \end{array} \right.$$

Si λ es un valor característico de la aplicación a con el vector propio x , λ^k es valor característico de la aplicación a^k con el mismo vector propio x .

Dado un polinomio

$$\psi(u) = c_k u^k + \dots + c_1 u + c_0 \quad (c_i \in \Delta)$$

consideremos la aplicación

$$\psi(a) = c_k a^k + \dots + c_1 a + c_0 I$$

Sea x un vector propio de a correspondiente al valor característico λ ; las relaciones (2) multiplicadas respectivamente por $c_0, c_1, \dots, c_k$ y sumadas miembro a miembro conducen a

$$\psi(a)x = \psi(\lambda)x.$$

Por consiguiente: Si λ es un valor característico de a con el vector propio x , y si $\psi(u)$ es un polinomio cualquiera con coeficiente en Δ , $\psi(\lambda)$ es valor característico de $\psi(a)$ con el vector propio x .

Los conocimientos sobre los valores característicos de una aplicación lineal a nos dan así información sobre los de la aplicación lineal $\psi(a)$. Si los valores $\psi(\lambda)$ son todos distintos, el procedimiento nos da todos los valores característicos de $\psi(a)$.

Hemos visto que el polinomio mínimo $m(u)$ y el polinomio característico $\varphi(u)$ de una aplicación lineal a tienen las mismas raíces (con órdenes de multiplicidad generalmente diferentes). Ahora bien, $m(u)$ es el polinomio de grado mínimo anulado por A , $m(A) = 0$, y todo polinomio anulado por A es múltiplo de $m(u)$. Es natural preguntarse si el polinomio característico tiene esa propiedad. La respuesta está dada por el teorema siguiente:

Teorema 2 (teorema de Hamilton-Cayley). — Toda matriz A verifica a su ecuación característica:

$$\varphi(A) = 0.$$

Ello resulta del lema general siguiente:

Lema. — Siendo $M_0, \dots, M_k$ matrices cuadradas de orden n sobre el cuerpo Δ y designando u una indeterminada, consideremos el polinomio

$$P(u) = M_k u^k + \dots + M_0 \in \mathcal{M}[u]$$

y supongamos que se tenga, para una matriz A , permutable con las M

$$P(A) = M_k A^k + \dots + M_0 = 0,$$

entonces, A también verifica la ecuación

$$\det P(u) = 0.$$

Señalemos primero que una vez demostrado el lema el teorema es inmediato, pues basta aplicar el lema al polinomio $P(u) = A - Iu$, en el cual $k = 1$, $M_0 = A$, $M_1 = -I$;

$$P(A) = 0 \quad \text{pues} \quad A - IA = A - A = 0$$

y como se tiene

$$\det P(u) = \det (A - Iu) = \varphi(u),$$

resulta

$$\varphi(A) = 0.$$

Demostremos el lema.

$P(u)$ es una matriz cuyos elementos son polinomios en u de grado $\leq k$ con coeficientes de Δ : en efecto, si $M_k = \| m_{ij}^k \|$, se tiene

$$P(u) = \| m_{ij}^k u^k + \dots + m_{ij}^0 \| = \| p_{ij} \|.$$

El determinante $\rho(u)$ de $P(u)$ es, pues, un polinomio en u de grado $\leq nk$, con coeficientes de Δ :

$$\rho(u) = \det P(u) = r_{nk} u^{nk} + \dots + r_0, \quad r_i \in \Delta.$$

Designemos por q_{ij} el menor de p_{ij} tomado con su signo exterior, y por Q la matriz de las q_{ji} (llamada a veces *matriz adjunta de P*).

Tenemos:

$$(3) \quad QP = \begin{vmatrix} \rho(u) & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \rho(u) \end{vmatrix} = \rho(u)I$$

Ahora bien, los elementos de Q son polinomios en u de grado $\leq (n-1)k$ y coeficientes de Δ y se puede escribir:

$$Q = N_{(n-1)k} u^{(n-1)k} + \dots + N_0$$

(donde cada N_i es una matriz- $n \times n$ sobre el cuerpo Δ).

La igualdad (3) se escribe

$$(3') \quad [N_{(n-1)k} u^{(n-1)k} + \dots + N_0][M_k u^k + \dots + M_0] = \rho(u)I \\ = r_{nk} I u^{nk} + \dots + r_0 I$$

y esta igualdad (3') subsiste si cambiamos la indeterminada u por la matriz A , puesto que ésta es permutable con las M_i por hipótesis; tenemos pues:

$$(4) \quad \rho(A) = [N_{(n-1)k} A^{(n-1)k} + \dots + N_0][M_k A^k + \dots + M_0] \\ = Q(A)P(A),$$

y, hecha la hipótesis, $P(A) = 0$, implica $\rho(A) = 0$.

Puesto que se anula para A , el polinomio característico es un múltiplo del polinomio mínimo $m(u)$:

$$\varphi(u) = m(u)\psi(u).$$

Ahora bien, sabemos ya que los dos polinomios tienen las mismas raíces; resulta ahora que éstas tienen en el polinomio característico un orden de multiplicidad por lo menos igual al que tienen en el polinomio mínimo. En particular, siempre que el polinomio característico $\varphi(u)$ tenga sólo raíces simples, el polinomio mínimo tiene también raíces simples, y coincide con el característico: $\varphi(u) = m(u)$.

Estudiemos el caso importante en que $m(u)$ tiene sólo raíces simples:

$$m(u) = (u - \lambda_1) \dots (u - \lambda_r), \quad \lambda_i \neq \lambda_j.$$

cada uno de los polinomios $f_k = u - \lambda_k$ es divisor de $m(u)$ y su grado es positivo. Hay, pues, un núcleo $\mathcal{N}_k$ de dimensión $\nu_k > 0$:

$$\mathcal{N}_k = \{x \in \mathcal{E}; (u - I\lambda_k)x = 0\}.$$

Elijamos una base del núcleo $\mathcal{N}_k$:

$$\mathcal{N}_k = (\varphi_{k1}, \dots, \varphi_{k\nu_k}).$$

Puesto que los factores lineales $u - \lambda_k$ son primos entre sí dos a dos, el espacio vectorial $\mathfrak{E}$ es la suma directa de los núcleos correspondientes:

$$\mathfrak{E} = \mathcal{N}_1 \oplus \mathcal{N}_2 \oplus \dots \oplus \mathcal{N}_r$$

y el espacio $\mathfrak{E}$ admite la base

$$\mathfrak{E} = (\varphi_{11}, \dots, \varphi_{1\nu_1}, \dots, \varphi_{r1}, \dots, \varphi_{r\nu_r}).$$

Con esta base, la matriz de la aplicación α se escribe:

$$A' = \begin{vmatrix} \lambda_1 & \dots & 0 & \dots & 0 & \dots & 0 \\ & \ddots & & & & & \\ 0 & \dots & \lambda_1 & \dots & 0 & \dots & 0 \\ & & \ddots & & & & \\ 0 & \dots & 0 & \dots & \lambda_r & \dots & 0 \\ & & & & \ddots & & \\ 0 & \dots & 0 & \dots & 0 & \dots & \lambda_r \end{vmatrix}$$

sus columnas son los vectores $\alpha\varphi$, transformados de los vectores de la base por α . Elegida la base, se obtiene una matriz *diagonal*, siendo los elementos de la diagonal los valores característicos escritos cada uno ν_k veces, donde ν_k es la dimensión del núcleo correspondiente y el orden de multiplicidad de la raíz λ_k de la ecuación característica. Tal matriz diagonal se escribe abreviadamente así

$$= [\lambda_1, \dots, \lambda_1; \dots; \lambda_r, \dots, \lambda_r]$$

Recíprocamente, si para una elección conveniente de la base $\mathfrak{E} = (a_1, \dots, a_n)$, la matriz A de α se puede poner en forma diagonal,

$$A = \begin{vmatrix} \mu_1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \mu_k & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \dots & \mu_n \end{vmatrix}$$

todas las raíces de la ecuación mínima son simples

En efecto, tenemos

$$(5) \quad \alpha a_k = \mu_k a_k$$

y, por consiguiente, si ponemos

$$f_k(u) = u - \mu_k \quad (\mu_k \in \Delta),$$

se tiene

$$f_k(\alpha) a_k = 0.$$

Puesto que a_k es un vector *no nulo* es un vector propio y μ_k es un valor característico, luego $u - \mu_k$ divide a $m(u)$.

Consideremos los μ_i que son distintos, sean $\mu_{i_1}, \mu_{i_2}, \dots, \mu_{i_r}$, y formemos el polinomio

$$g(u) = (u - \mu_{i_1}) \dots (u - \mu_{i_r});$$

producto de factores lineales primos entre sí dos a dos y divisores todos de $m(u)$, luego $g(u)$ divide a $m(u)$.

Vamos a ver que $m(u)$ divide a $g(u)$, y para ello que $g(\alpha)$ es la aplicación nula:

$$g(\alpha) = (\alpha - \mu_{i_1} I) \dots (\alpha - \mu_{i_r} I);$$

los factores son *permutables*, luego se puede poner al final el factor $\alpha - \mu_k$ y entonces, según (5), se tiene

$$g(\alpha) a_k = \dots (\alpha - \mu_k) a_k = 0;$$

y siendo esto verdad para *cada* vector fundamental a_k , resulta que

$$g(\alpha) = 0$$

y en consecuencia $m(u)$ divide a $g(u)$, de donde, finalmente, $m(u) = g(u)$, polinomio que tiene simples todos sus ceros. Podemos enunciar:

Teorema 3. — *Para que por una elección conveniente de la base se pueda poner una matriz en forma diagonal, es necesario y suficiente que la ecuación mínima de esta matriz tenga solamente raíces simples.*

Poniéndonos en el caso del teorema precedente, volvamos a la proposición

directa.

Podemos utilizar la matriz diagonal $A' = [\lambda_1, \dots, \lambda_1; \dots; \lambda_r, \dots, \lambda_r]$ para formar el polinomio característico, lo que da

$$\varphi(u) = (u - \lambda_1)^{p_1} \dots (u - \lambda_r)^{p_r}$$

Si estamos en el caso más particular en que el polinomio característico tiene todos sus ceros simples, todos los p_k son iguales a 1 y cada núcleo $\mathcal{N}_k$ tiene un solo vector de base. Luego:

Corolario. — *Cuando el polinomio característico tiene todos sus ceros simples, a cada uno de estos ceros corresponde un vector propio, definido a menos de un factor no nulo, y estos n vectores forman una base del espacio $\mathcal{E}$. Elegida esta base, la matriz de la aplicación lineal se reduce a la forma diagonal.*

CAPÍTULO X

CUERPOS. ECUACIONES ALGEBRAICAS

§ 1. Extensiones simples

Sea $K = k(\alpha)$ una *extensión simple* de un cuerpo k (cap. IV, § 3). Supondremos K conmutativo y, por ende, también k (en general, salvo en los § 4 y 9, los cuerpos considerados en este capítulo serán conmutativos).

A cada polinomio $f(x)$ del anillo $k[x]$, asociemos su valor $f(\alpha)$ para $x = \alpha$. La aplicación así definida,

$$(\theta) \quad f(x) \rightarrow f(\alpha)$$

es un *homomorfismo* que aplica el anillo de polinomios $k[x]$ sobre el anillo $k[\alpha]$ ($\subseteq K$):

$$(\theta) \quad k[x] \sim k[\alpha].$$

Las constantes $a \in k$ coinciden con su imagen respectiva.

Según el teorema de homomorfismo para los anillos (cap. IV, § 7) tendremos el *isomorfismo*

$$k[x]/\mathfrak{a} \simeq k[\alpha]$$

donde $\mathfrak{a}$, *núcleo* del homomorfismo θ , es el ideal de polinomios $f \in k[x]$ nulos para $x = \alpha$.

En este isomorfismo, cada elemento a de k es también su propia imagen, hecho que expresaremos diciendo que se trata de un *isomorfismo sobre k* .

Puesto que $k[\alpha]$ es un dominio de integridad (por ser subanillo de un cuerpo), el anillo isomorfo $k[x]/\mathfrak{a}$ lo es también y, en consecuencia, $\mathfrak{a}$ es un *ideal primo*.

$k(\alpha)$ es una expresión polinómica $f(\alpha)$ en α ; si se reemplaza $f(x)$ por su resto $r(x)$ módulo $p(x)$

$$f(x) = p(x)q(x) + r(x) \text{ grado de } r < \nu$$

se obtiene

$$(2) \quad \xi = f(\alpha) = r(\alpha) = c_0 + c_1\alpha + \dots + c_{\nu-1}\alpha^{\nu-1} \quad (c_i \in k)$$

Esta representación es única (puesto que ν es mínimo). Enunciaremos:

Teorema 1. — *Una extensión algebraica simple $k(\alpha)$ de un cuerpo k es isomorfa sobre k con el cuerpo de las clases residuales $k[x]/(p(x))$ donde $p(x)$ es un polinomio irreducible sobre k , de grado ν [$\nu \geq 2$ si $k(\alpha) \neq k$]. Todo elemento ξ de $k(\alpha)$ admite una expresión polinómica en α de grado $\leq \nu - 1$, con coeficientes de k , y esta representación (2) es única.*

Son oportunos dos complementos importantes del teorema precedente, puntos de partida para otros resultados.

1.º La existencia y unicidad de la representación de cada elemento de $k(\alpha)$ en la forma

$$(2) \quad \xi = c_0 + c_1\alpha + \dots + c_{\nu-1}\alpha^{\nu-1} \quad (c_i \in k)$$

significan que la extensión algebraica simple $k(\alpha)$ es un espacio vectorial de dimensión ν sobre el cuerpo k , y que para este espacio vectorial se tiene la base

$$(\alpha^0 = e, \alpha, \dots, \alpha^{\nu-1}).$$

Además, los elementos de esta base se multiplican según la ley (asociativa)

$$\alpha^r \cdot \alpha^s = \sum_{t=0}^{\nu-1} \gamma_{r,s,t} \alpha^t, \quad \gamma_{r,s,t} \in k,$$

donde el segundo miembro se obtiene reemplazando x por α en el resto de la división de x^{r+s} por $p(x)$; $k(\alpha)$ es, pues, un álgebra asociativa sobre k .

De un modo general, todo supercuerpo k' de un cuerpo k es un espacio vectorial sobre k (cap. VIII, § 1).

La dimensión de k' considerado como espacio vectorial sobre k es, por definición, el grado de k' , extensión de k , y se indica

$$(k' : k).$$

El grado puede ser *finito* o *infinito*. En el caso de una extensión simple $k' = k(\alpha)$, el grado $(k' : k)$ es finito si la extensión es algebraica, y es infinito si la extensión es trascendente. Sabemos, en efecto, que toda extensión algebraica simple es de grado finito ν (grado del polinomio característico de α) y recíprocamente si $k(\alpha)$ es de grado finito ν y los $\nu + 1$ elementos $e = \alpha^0, \alpha, \dots, \alpha^\nu$ serán linealmente dependientes sobre k , y habrá elementos a_i de k no todos nulos tales que

$$a_0 + a_1\alpha + \dots + a_\nu\alpha^\nu = 0$$

es decir, α verifica la ecuación algebraica

$$p(x) = 0 \quad \text{donde, } p(x) = a_0 + a_1x + \dots + a_\nu x^\nu \in k[x], \quad p(x) \neq 0.$$

2.º El polinomio $p(x)$ del anillo $k[x]$, polinomio característico de la extensión algebraica simple $k(\alpha)$, admite en $k(\alpha)$, y en todo supercuerpo K de $k(\alpha)$, la raíz α , y es irreducible sobre k . Como sabemos (cap. IV, § 7) esto exige que $p(x)$ sea divisible por $x - \alpha$:

$$p(x) = (x - \alpha)p_1(x)$$

donde $p_1(x)$ es un polinomio con coeficientes en $k(\alpha)$ ($\subseteq K$).

Tenemos, pues, en el anillo $K[x]$ ($k \subset k(\alpha) \subseteq K$) una descomposición de la forma

$$p(x) = (x - \alpha_1) \dots (x - \alpha_r) q_1(x) \dots q_s(x) \quad (r \geq 1, s \geq 0)$$

donde $\alpha_1 = \alpha$ y los eventuales q_i , son polinomios irreducibles sobre K de grado > 1 . Las α_i son los ceros de $p(x)$ sobre K .

§ 2. Cuerpo de ruptura. Cuerpo de descomposición

El problema inverso es importante. En vez de darnos la extensión simple $k(\alpha)$ y estudiarla mediante su polinomio característico $p(x)$, partamos de un polinomio $f(x)$ irreducible sobre k en el anillo $k[x]$, e intentemos construir una extensión simple $k' = k(\zeta)$ de k en la cual $f(x)$ admita ζ como cero. Una extensión simple tal, se llama *cuerpo de ruptura* del polinomio $f(x)$. El método para construirlo, debido a Cauchy, es el de *adjunción simbólica*.

Puesto que f es irreducible sobre k , el ideal (f) en el anillo $k[x]$ es máximo y el anillo cociente $k[x]/(f)$ es un cuerpo Σ ; dos constantes (es decir, dos elementos de k) si son distintas no serán congruentes módulo f , luego pertenecerán a dos clases distintas, y en consecuencia el cuerpo $\Sigma = k[x]/(f)$ contiene un subcuerpo $\bar{k}$ isomorfo con k , conjunto de las clases módulo f que contienen a las constantes. Identificaremos $\bar{k}$ con k , y consideraremos a Σ como un supercuerpo de k .

Si $\zeta \in \Sigma$ es la clase a que pertenece el polinomio x , el polinomio $\varphi = r_0 + r_1x + \dots + r_nx^n$ pertenecerá a la clase $\bar{\varphi} = r_0 + r_1\zeta + \dots + r_n\zeta^n$.

Las clases $\bar{\varphi} \in \Sigma$ son, pues, *expresiones polinómicas* en ζ , y se tiene

$$\Sigma \subseteq k[\zeta] \subseteq k(\zeta) \subseteq \Sigma$$

por lo que vale la igualdad y Σ es una *extensión simple* de k :

$$\Sigma = k(\zeta).$$

El polinomio dado $f = a_0 + a_1x + \dots + a_mx^m$, pertenece a la clase 0 , $0 \in \Sigma$, pero también, según lo que precede a la clase

$$a_0 + a_1\zeta + \dots + a_m\zeta^m.$$

En Σ se tiene la igualdad

$$a_0 + a_1\zeta + \dots + a_m\zeta^m = 0,$$

luego la extensión simple $\Sigma = k(\zeta)$ es *algebraica* y en ella el elemento ζ de Σ es un cero de f . Como f es irreducible sobre k , es f el polinomio característico de Σ (o de ζ) salvo un factor a_n , coeficiente director de f . El cuerpo Σ es un cuerpo de ruptura de f .

Dos extensiones algebraicas simples $k(\alpha)$, $k(\beta)$ contenidas en sendos supercuerpos K , L de k , pueden tener *el mismo polinomio característico* $f(x)$ y constituir dos cuerpos de ruptura de este polinomio. Pero entonces ambas son isomorfas con el cuerpo $k[x]/(f)$, y por lo tanto isomorfas entre sí en el isomorfismo

$$\xi = c_0 + c_1\alpha + \dots + c_{p-1}\alpha^{p-1} \rightarrow \eta = c_0 + c_1\beta + \dots + c_{p-1}\beta^{p-1},$$

que es un isomorfismo sobre k . De este modo:

Teorema 1. — *Dos cuerpos de ruptura sobre k de un polinomio irreducible $f(x)$ del anillo $k[x]$, son isomorfos sobre k .*

Ejemplos. — 1. El método de adjunción simbólica permite definir de modo completamente algebraico el cuerpo de ruptura $\mathbf{Q}(\sqrt{2})$ del polinomio $x^2 - 2$ sobre el cuerpo de los racionales $\mathbf{Q}$, y en particular el número $\sqrt{2}$; y, análogamente, el cuerpo de ruptura $\mathbf{R}(i)$ del polinomio $x^2 + 1$ sobre el cuerpo de los números reales, es decir, los números complejos.

2. Indicando, como siempre por $\mathbf{Q}$ el cuerpo de los racionales, la extensión simple

$$\Sigma = \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{R}$$

es un cuerpo de ruptura del polinomio $p(x) = x^3 - 2$, irreducible sobre $\mathbf{Q}$. Sobre Σ , se tendrá la descomposición

$$f(x) = (x - \sqrt[3]{2}) (x^2 + x\sqrt[3]{2} + \sqrt[3]{4})$$

cuyo segundo factor es irreducible sobre Σ y también sobre $\mathbf{R}$. Aquí el pasar al cuerpo de ruptura ha hecho aparecer sólo un factor lineal.

Según el teorema 2, los cuerpos $\mathbf{Q}(\sqrt[3]{2})$ y $\mathbf{Q}(j\sqrt[3]{2})$, donde $j = (-1 + i\sqrt{3})/2$, son isomorfos sobre $\mathbf{Q}$.

Si sobre un cuerpo de ruptura $\Sigma_1 = k(\zeta_1)$, un polinomio f del anillo $k[x]$ irreducible sobre k se descompone en factores irreducibles que no son todos lineales, resulta natural considerar un cuerpo de ruptura $\Sigma_2 = \Sigma_1(\zeta_2)$ de un tal polinomio factor y realizar la descomposición de f en factores irreducibles sobre Σ_2 : en ésta aparecen más factores lineales que en la descomposición sobre Σ_1 . La reiteración de este procedimiento conduce pues, al cabo de un número finito λ de operaciones a un cuerpo Σ_λ sobre el cual f se descompone enteramente en factores lineales:

Teorema 2. — *Dado un polinomio $f \in k[x]$ irreducible sobre k , existe una extensión Σ_λ de k obtenida por una sucesión de λ extensiones algebraicas simples, sobre la que $f(x)$ se descompone totalmente en factores lineales.*

Sean k un cuerpo y $f(x)$ un polinomio del anillo $k[x]$.

Definición. — Dados k y $f(x) \in k[x]$ que no se descompone totalmente en factores lineales sobre k , se llama cuerpo de descomposición ¹ de f (sobre k), un supercuerpo Δ de k tal que

- 1.º Sobre Δ , f se descompone totalmente en factores lineales;
- 2.º Sobre cualquier cuerpo intermedio Σ (si es que existe)

$$k \subset \Sigma \subset \Delta \quad (\text{estrictamente}),$$

f no se puede descomponer en factores todos lineales.

Observación 1. — Si f , sobre k , se descompone ya en factores lineales se tomará $\Delta = k$. En este caso puede ser interesante ver si se podría reemplazar k por su menor subcuerpo k' que contenga a todos los coeficientes de f , (k' será la intersección de todos los subcuerpos de k que contienen a dichos coeficientes a_i), y buscar un cuerpo de descomposición Δ' asociado a k' , supercuerpo minimal de k' sobre el que f se descomponga en factores lineales.

¹ Diversos autores dicen cuerpo (o campo) raíz en vez de cuerpo de descomposición. (N. del T.)

Ejemplo:

$$f = x^2 - 2, \quad k = R, \quad \Delta = R.$$

$$k' = Q, \quad \Delta' = Q(\sqrt{2}).$$

Observación 2.—Por esta definición Δ es evidentemente el mismo para f que para el cociente f_1 de f por los factores lineales de f en $k[x]$.

Es fácil demostrar que $k(\alpha_1, \dots, \alpha_n) = \Delta$, donde las α_i son los ceros de f en el supercuerpo Σ_λ construido en § 1, es un cuerpo de descomposición sobre k .

En efecto, sea $k \subset \Sigma \subseteq \Delta$ y supongamos que se tenga una descomposición de f

$$(1) \quad f(x) = b(x - \beta_1) \dots (x - \beta_n) \quad \beta_i \in \Sigma$$

con factores lineales en $\Sigma[x]$. Puesto que $\Sigma[x] \subseteq \Delta[x]$, esta descomposición coincide con la

$$(2) \quad f(x) = a(x - \alpha_1) \dots (x - \alpha_n) \quad \alpha_i \in \Delta$$

en $\Delta[x]$, ya que $\Delta[x]$ es un anillo con factorización única. Por consiguiente las α_i pertenecen a Σ y $\Delta = k(\alpha_1, \dots, \alpha_n) = \Sigma$ (cap. IV, § 6, teor. 5).

Demostremos que recíprocamente, todo cuerpo de descomposición Δ puede obtenerse a partir de k por la formación sucesiva de extensiones simples en número finito.

Siendo $\Delta (\supset k)$ un cuerpo de descomposición de $f(x) \in k[x]$, sean

$$(3) \quad f(x) = p_1(x)p_2(x) \dots p_r(x) \quad \text{en } k[x],$$

$$(4) \quad f(x) = a(x - \alpha_1) \dots \quad \text{en } \Delta[x], \alpha_i \in \Delta$$

las descomposiciones de f en factores irreducibles p_i sobre k , y en factores lineales en $\Delta[x]$.

Siendo $\Delta[x]$ un anillo factorial, se tiene (con notaciones convenientes)

$$p_1(x) = c(x - \alpha_1) \dots$$

y $\alpha_1 \notin k$ si es grado de $p_1 > 1$. Entonces $k(\alpha_1)$ será una extensión simple de k , necesariamente algebraica, ya que $p_1(\alpha_1) = 0$.

El polinomio $p_1(x)$ pertenece al ideal $\mathfrak{a}_1$ de los polinomios de $k[x]$ nulos para $x = \alpha_1$, que es el ideal engendrado por el polinomio característico de α_1 , $q_1(x)$. Como p_1 es irreducible sobre k , q_1 sólo difiere de él en un factor constante; las congruencias $f \equiv g(p_1)$ y $f \equiv g(q_1)$ se verifican simultáneamente, y tendremos:

$$k(\alpha_1) \simeq k[x]/q_1 = k[x]/p_1.$$

Reemplazando k por $k_1 = k(\alpha_1)$, se tiene una descomposición de f en $k_1[x]$ análoga a (3): si los nuevos factores irreducibles p_i^* son todos lineales se ha concluido, $\Delta = k_1$; si no, se volverá a empezar sobre un factor p_1^* irreducible de grado > 1 . Después de un número finito λ de operaciones se obtendrá $\Delta = k_\lambda$ con $k_{i+1} = k_i(\alpha_{i+1})$, siendo $\alpha_1, \dots, \alpha_\lambda$ ciertos ceros de f en Δ .

Ahora nos proponemos demostrar que *dos cuerpos de descomposición del polinomio $f(x) \in k[x]$ son isomorfos*.

Definición. — Dados dos anillos o dos cuerpos $k, \bar{k}$ isomorfos en un isomorfismo φ

$$(\varphi) \quad k \simeq \bar{k} \quad \bar{k} = \varphi k$$

y dos superanillos o supercuerpos respectivos $K, \bar{K}$, se dice que un isomorfismo Φ de K sobre $\bar{K}$

$$(\Phi) \quad K \simeq \bar{K} \quad \bar{K} = \Phi K$$

es *prolongación* de φ (o *prolonga* a φ), si su restricción a k coincide con φ :

$$\Phi x = \varphi x \quad \forall x \in k$$

Más generalmente, si $K, \bar{K}$ son dos *extensiones* de $k, \bar{k}$, respectivamente, es decir, contienen dos anillos o dos subcuerpos $k', \bar{k}'$ isomorfos con $k, \bar{k}$, en los isomorfismos $\eta, \bar{\eta}$:

$$k' \subseteq K, \quad k' \simeq k \quad (\eta), \quad \bar{k}' \subseteq \bar{K}, \quad \bar{k}' \simeq \bar{k} \quad (\bar{\eta}),$$

k' y $\bar{k}'$ resultan isomorfos en el isomorfismo $\varphi' = \bar{\eta}^{-1}\varphi\eta$:

$$\bar{k}' = \varphi' k',$$

y se dirá que Φ prolonga a φ si

$$\Phi x = \varphi' x \quad \forall x \in k'$$

es decir, si la restricción de Φ al subconjunto k' es φ'

Casos particulares. — I. Sea φ la identidad (luego $\bar{k} = k$). En tal caso Φ es un isomorfismo sobre k , o k -isomorfismo.

II. Dado el isomorfismo

$$(\varphi) \quad k \simeq \bar{k}$$

consideremos los anillos

$$A_1 = k[x], \quad \bar{A} = \bar{k}[x]$$

La aplicación

$$a_0 + a_1x + \dots + a_nx^n \rightarrow \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n$$

donde $\bar{a}_i = \varphi a_i$, es un isomorfismo Ψ que aplica el anillo A sobre $\bar{A}$ y prolonga a φ .

III. Si $f = f_1f_2$, $\Psi(f) = \bar{f} = \bar{f}_1\bar{f}_2$, donde $\bar{f}_i = \Psi(f_i)$ e inversamente (considerando el isomorfismo inverso Ψ^{-1} que prolonga al φ^{-1}): luego, los polinomios irreducibles de los dos anillos A y $\bar{A}$ se corresponden biunívocamente.

Establecido esto, sean p y $\bar{p} = \Psi(p)$ dos de tales polinomios irreducibles correspondiéndose. Consideremos los cuerpos de ruptura

$$\rho = k[x]/(p) \quad \bar{\rho} = \bar{k}[x]/(\bar{p})$$

definidos como anillos de las clases de restos módulo p , o $\bar{p}$. Una clase $C \in k[x]/(p)$ está formada de polinomios $f, g, \dots$ congruentes dos a dos módulo p : $f - g = qp$; sus imágenes $\Psi(f), \Psi(g), \dots$ son congruentes módulo $\bar{p} = \Psi(p)$ e inversamente, luego constituyen una clase $\bar{C} \in \bar{k}[x]/(\bar{p})$; al poner $\bar{C} = \Psi^*(C)$, definimos ¹ una aplicación biyectiva de ρ sobre $\bar{\rho}$, y esta aplicación respeta la adición y la multiplicación de clases, puesto que Ψ es un isomorfismo.

Así, los dos cuerpos de ruptura $k[x]/(p) = \rho$, $\bar{k}[x]/(\bar{p}) = \bar{\rho}$, son isomorfos en el isomorfismo Ψ^* prolongación del isomorfismo dado φ .

¹ Definimos, $\bar{C} = \Psi^*(C)$ si $\bar{C} \ni \bar{f} = \Psi(f)$ donde $f \in C$.

Luego Ψ^* es un isomorfismo que aplica ρ sobre $\bar{\rho}$. Además, este isomorfismo prolonga φ . En efecto, sea a un elemento de k ; la constante $a \in k[x]$ pertenece, módulo p , a una clase C cuya imagen $\Psi^*(C) = \bar{C}$ es la clase que contiene la constante $\Psi(a)$, $\Psi(a) = \varphi(a) \in \bar{k}$.

IV. Consideremos ahora dos cuerpos de ruptura cualesquiera $k(\alpha)$ de p y $\bar{k}(\bar{\alpha})$ de $\bar{p}$; sabemos ya que $k(\alpha)$ es isomorfo con k en un isomorfismo σ sobre k (o k -isomorfismo), y lo análogo para $\bar{k}(\bar{\alpha})$: tendremos, pues, la sucesión de isomorfismos.

$$k(\alpha) \underset{\sigma}{\simeq} k[x]/(p) \underset{\Psi^*}{\simeq} \bar{k}[x]/(\bar{p}) \underset{\bar{\sigma}^{-1}}{\simeq} \bar{k}(\bar{\alpha}).$$

Entonces $\varphi_1 = \bar{\sigma}^{-1}\Psi^*\sigma$ es un isomorfismo que aplica $k(\alpha)$ sobre $\bar{k}(\bar{\alpha})$; φ_1 prolonga a φ , puesto que, si $a \in k$, $\sigma(a)$ es la clase C módulo p que contiene a a , $\Psi^*(C) = \bar{C}$ es la clase que contiene a $\Psi(a) = \varphi(a) \in \bar{k}$ y $\bar{\sigma}^{-1}\bar{C}$ es el elemento $\varphi(a)$ de $\bar{k}$.

Además, las imágenes sucesivas de α son $\sigma(\alpha) = X$, clase módulo p que contiene a x ¹, $\Psi^*\sigma(\alpha) = \bar{X}$, clase que contiene a x módulo $\bar{p}$, y

$$\varphi_1(\alpha) = \bar{\sigma}^{-1}\Psi^*\sigma(\alpha) = \bar{\sigma}^{-1}(\bar{X}) = \bar{\alpha}.$$

Con esto resulta que, si

$$\xi = c_0 + c_1\alpha + \dots + c_{p-1}\alpha^{p-1} \quad (c_i \in k)$$

es la representación canónica de un elemento $\xi \in k(\alpha)$, su transformado vendrá representado por

$$\varphi_1(\xi) = \bar{c}_0 + \bar{c}_1\bar{\alpha} + \dots + \bar{c}_{p-1}\bar{\alpha}^{p-1}$$

donde, naturalmente,

$$\bar{c}_i = \varphi(c_i) \in \bar{k}.$$

Esta conclusión se resume en el

Teorema 3. — *Los dos cuerpos de ruptura $k(\alpha)$ de p y $\bar{k}(\bar{\alpha})$ de $\bar{p} = \Psi(p)$ son isomorfos en un isomorfismo φ_1 prologación de φ , φ_1 , definido por $\varphi_1 = \bar{\sigma}^{-1}\Psi^*\sigma$ o por*

$$\xi = c_0 + c_1\alpha + \dots + c_{p-1}\alpha^{p-1} \rightarrow \varphi_1(\xi) = \bar{c}_0 + \bar{c}_1\bar{\alpha} + \dots + \bar{c}_{p-1}\bar{\alpha}^{p-1},$$

con $\bar{c}_i = \varphi(c_i)$.

Consideremos ahora un polinomio cualquiera $f(x) \in k[x]$ y sea, con las nota-

¹ Recordemos que el isomorfismo σ se ha definido a partir del isomorfismo de anillos $k[x] \simeq k[\alpha]$ asociando a $f(x)$ su valor $f(\alpha)$ para $x = \alpha$; el polinomio x tiene por imagen α en tal isomorfismo.

ciones precedentes, $f(x) = \Psi(f)$ su imagen en $\bar{k}[x]$ donde $\bar{k} = \varphi(k)$ y Ψ prolonga a φ .

Teorema 4. — *Dos cuerpos de descomposición Δ de f y $\bar{\Delta}$ de $\bar{f}$ son isomorfos en un isomorfismo Φ prolongación de φ .*

1.º Supongamos primero que todos los ceros de f estén en k , luego $\Delta = k$:

$$f(x) = a(x - \alpha_1) \dots (x - \alpha_n) \quad a \in k, \alpha_i \in k$$

de donde, para $\bar{f} = \Psi(f)$, vale la descomposición

$$\bar{f}(x) = \bar{a}(x - \bar{\alpha}_1) \dots (x - \bar{\alpha}_n)$$

donde

$$\bar{a} = \varphi(a) \in \bar{k}, \quad \bar{\alpha}_i = \varphi(\alpha_i) \in \bar{k}.$$

Resulta también $\bar{\Delta} = \bar{k}$, y el isomorfismo buscado Φ no es otro que φ .

2.º Supongamos ahora que $f(x)$, de grado n , tenga exactamente m ceros α_i fuera de k ($0 < m \leq n$); y demostremos el teorema por recurrencia, suponiéndolo verdadero para todo polinomio de $k[x]$ que tenga menos de m raíces fuera de k . Por 1.º, el teorema es cierto para $m = 0$; no ha lugar a examinar el caso $m = 1$, puesto que un polinomio de $k[x]$ no puede tener una sola raíz fuera de k .

Sea

$$(5) \quad f = p_1 \dots p_r$$

la descomposición de f en $k[x]$ en factores irreducibles p_i , donde uno al menos, p_1 , es de grado $n_1 > 1$.

Aplicando el isomorfismo de anillos Ψ , se pasa de (5) a

$$(6) \quad \Psi(f) = \bar{f} = \bar{p}_1 \dots \bar{p}_r$$

donde $\Psi(p_i) = \bar{p}_i$ es irreducible y el grado de $\bar{p}_1$ es n_1 .

Sean $\alpha_1 \in \Delta$ un cero de p_1 , y $\bar{\alpha}_1 \in \bar{\Delta}$ un cero de $\bar{p}_1 = \Psi(p_1)$.

Como se ha visto más arriba, $k(\alpha_1) (\subseteq \Delta)$ es un cuerpo de ruptura de $p_1(x)$; e igualmente, $\bar{k}(\bar{\alpha}_1) (\subseteq \bar{\Delta})$ es un cuerpo de ruptura de $\bar{p}_1 = \Psi(p_1)$. Por el teorema 3 existe un isomorfismo φ_1 que prolonga φ y aplica $k(\alpha_1) = k_1$ sobre $\bar{k}(\bar{\alpha}_1) = \bar{k}_1$.

Como f tiene menos de m raíces fuera de k_1 , existe por la hipótesis de recurrencia, un isomorfismo Φ entre los cuerpos de descomposición $\Delta, \bar{\Delta}$:

$$(\Phi) \quad \Delta \simeq \bar{\Delta}, \quad \bar{\Delta} = \Phi(\Delta).$$

Como Φ , prolonga a φ_1 y, por consiguiente, a φ , es el isomorfismo buscado.

Para el caso particular $\bar{k} = k$, puede enunciarse:

Teorema 5. — *Dos cuerpos de descomposición Δ , Δ' de un mismo polinomio $f \in k[x]$ son isomorfos sobre k .*

Se dirá, pues, *el cuerpo* (y no *un cuerpo*) de descomposición de un polinomio $f(x) \in k[x]$; entendiéndose que este cuerpo está definido salvo isomorfismos.

§ 3. Extensiones finitas, elementos algebraicos

Sea K un supercuerpo de k ; la dimensión de K considerado como espacio vectorial sobre k ha sido llamada *grado* de K (con relación a k); si este grado $(K : k)$ es finito, se dice que K es una *extensión finita* de k , o mejor una *extensión de dimensión finita* o de *grado finito*. Si $(K : k) = \infty$, se dice que K es *extensión infinita* de k .

Se dice, por otra parte, que un supercuerpo L de k es una *extensión algebraica* de k si todo elemento α de L es algebraico sobre k , es decir, es cero de un polinomio $f(x) \in k[x]$.

Teorema. 1 — *Toda extensión finita K de k es una extensión algebraica de k .*

Sea $(K : k) = \nu$. Cualquiera que sea $\alpha \in K$, los $\nu + 1$ elementos $e = \alpha^0, \alpha, \dots, \alpha^\nu$ de K no son linealmente independientes sobre k : se tendrá, pues, una relación de la forma

$$a_0 + a_1\alpha + \dots + a_\nu\alpha^\nu = 0, \quad a_i \in k,$$

donde las a_i no son todas nulas; es decir, que α es algebraico sobre k .

Nota. — El recíproco no es cierto: el cuerpo A de todos los números algebraicos no es extensión finita del cuerpo $\mathbb{Q}$ de los racionales.

Teorema 2. — *Sean K_2 un supercuerpo de K_1 , K_3 un supercuerpo de K_2 , y por consiguiente de K_1 :*

$$K_1 \subseteq K_2 \subseteq K_3.$$

Se tiene:

$$(K_3 : K_1) = (K_3 : K_2)(K_2 : K_1)$$

N. B. — Esta propiedad justifica la notación empleada para el grado. El teorema vale tanto para las extensiones finitas como para las infinitas.

Demostración.

1.º Si $a_1, \dots, a_r$ son r elementos de K_3 linealmente independientes sobre K_2 lo que exige $r \leq (K_3 : K_2)$, y si $b_1, \dots, b_s$ son s elementos de K_2 linealmente independientes sobre K_1 , lo que exige $s \leq (K_2 : K_1)$, los rs elementos $a_i b_j$ de K_3 son linealmente independientes sobre K_1 .

Sea en efecto

$$\sum_{i,j} \lambda_{ij} a_i b_j = 0 \quad \lambda_{ij} \in K_1,$$

Esta igualdad se escribe

$$\sum_i \left(\sum_j \lambda_{ij} b_j \right) a_i = 0, \quad \text{donde} \quad \sum_j \lambda_{ij} b_j \in K_2.$$

Puesto que las a_i son linealmente independientes sobre K_2 , resulta

$$\sum_j \lambda_{ij} b_j = 0 \quad (i = 1, \dots, r)$$

pero, siendo las b_j linealmente independientes sobre K_1 , se tiene:

$$\lambda_{ij} = 0 \quad (i = 1, \dots, r; j = 1, \dots, s)$$

como queríamos demostrar.

Se tiene pues

$$rs \leq (K_3 : K_1) \quad \forall \begin{cases} r \leq (K_3 : K_2), \\ s \leq (K_2 : K_1). \end{cases}$$

$(K_3 : K_1)$ es pues infinito cuando uno al menos de los grados $(K_2 : K_1)$, $(K_3 : K_2)$ es infinito y, en este caso, el teorema queda demostrado.

2.º Supongamos ahora los dos grados $(K_3 : K_2)$ y $(K_2 : K_1)$ finitos y sean éstos $r = (K_3 : K_2)$, $s = (K_2 : K_1)$; tenemos

$$(K_3 : K_2) (K_2 : K_1) \leq (K_3 : K_1).$$

Pero para un elemento cualquiera x de K_3 , se tiene, puesto que las a_i constituyen una base de K_3 considerado como espacio vectorial sobre K_2 :

$$x = \sum_{i=1}^r \alpha_i a_i, \quad \alpha_i \in K_2.$$

Del mismo modo, siendo $(b_1, \dots, b_s)$ una base de K_2 sobre K_1 , se tiene

$$a_i = \sum_{j=1}^s \beta_{ij} b_j, \quad \beta_{ij} \in K_1$$

de donde

$$x = \sum_{i=1}^r \sum_{j=1}^s \beta_{ij} a_i b_j.$$

Los rs elementos $a_i b_j$ de K_3 engendran a K_3 como espacio vectorial sobre K_1 ; como son linealmente independientes, forman una base y tenemos:

$$(1) \quad (K_3 : K_1) = (K_3 : K_2) (K_2 : K_1).$$

Para una serie de n cuerpos encajados

$$K_1 \subset K_2 \subset \dots \subset K_n,$$

se tiene $(K_n : K_1) = (K_n : K_{n-1}) (K_{n-1} : K_{n-2}) \dots (K_2 : K_1)$

(demostración inmediata por recurrencia sobre n). Además, si k es subcuerpo de un cuerpo K , un elemento $\alpha \in K$ algebraico sobre k es evidentemente algebraico sobre un cuerpo L intermedio, pero el polinomio característico de α no es necesariamente el mismo en k y en L . (El polinomio de $k[x]$ anulado por α es un polinomio de $L[x]$; el polinomio característico de α sobre L será divisor del antedicho, luego el grado de α sobre L es inferior o igual a su grado sobre k).

Si $K = k(\alpha_1, \dots, \alpha_n)$ es una extensión de k obtenida por la adjunción de un número finito de elementos α_i algebraicos sobre k , pongamos

$$k_i = k(\alpha_1, \dots, \alpha_i) = k_{i-1}(\alpha_i) \quad \text{con} \quad k_0 = k, k_n = K;$$

α_i es algebraico sobre k , y por consiguiente sobre el cuerpo intermedio k_{i-1} ; sea ν_i el grado (finito) de k_i sobre k_{i-1} :

$$\nu_i = (k_i : k_{i-1})$$

Tendremos

$$(K : k) = (k_n : k_0) = \prod_{i=1}^n (k_i : k_{i-1}) = \nu_1 \dots \nu_n$$

y $K = k(\alpha_1, \dots, \alpha_n)$ es una extensión finita de k . Así

Teorema 3. — *Un supercuerpo $K = k(\alpha_1, \dots, \alpha_n)$ de k , obtenido por la adjunción de un número finito de elementos α_i algebraicos sobre k , es extensión finita de k . En particular, el cuerpo de descomposición Δ de un polinomio $f(x) \in k[x]$ es extensión finita de k (y al construirlo se ve cómo determinar su grado sobre k).*

Teorema 3'. — *Recíprocamente, toda extensión finita K de k puede obtenerse agregando a k un número finito de elementos algebraicos.*

Sea $(\theta_1, \dots, \theta_n)$ una base de K , como espacio vectorial sobre k ; $h = (K : k)$, y todo elemento ξ de K es de la forma

$$\xi = a_1\theta_1 + \dots + a_n\theta_n, \quad a_i \in k$$

luego $K = k(\theta_1, \dots, \theta_n)$. Además (por el teorema 1) cada θ_i es algebraico sobre k ; la proposición está pues demostrada.

En resumen, hay identidad entre la noción de extensión finita (es decir, de dimensión finita o de grado finito) y la de extensión obtenida por la agregación de un número finito de elementos algebraicos. También es frecuente designarla por "extensión algebraica finita".

En un supercuerpo Σ de k , supongamos que existen dos elementos α_1, α_2 algebraicos sobre k . Entonces el cuerpo intermedio $k(\alpha_1, \alpha_2)$ es, por el teorema 3, una extensión finita de k . Los elementos $\alpha_1 + \alpha_2, \alpha_1 - \alpha_2, \alpha_1\alpha_2$ y α_1/α_2 ($\alpha_2 \neq 0$) pertenecen a $k(\alpha_1, \alpha_2)$, luego son algebraicos sobre k , por el teorema 1. Así:

Teorema 4. — *La suma, la diferencia, el producto, el cociente de elementos algebraicos sobre k son también algebraicos sobre k .*

Se tiene además una propiedad de transferencia. Sea Σ un supercuerpo de K y K un supercuerpo de k :

Teorema 5. — *Si un elemento α de Σ es algebraico sobre K y si K es extensión algebraica de k , α es algebraico sobre k .*

Consideremos un polinomio $f(x)$ de $K[x]$ anulado por α :

$$f(\alpha) = 0, \quad f(x) = a_0 + a_1x + \dots + a_nx^n, \quad a_i \in K.$$

No suponemos que K es extensión finita de k . Pero basta considerar el cuerpo intermedio

$$L = k(a_0, a_1, \dots, a_n).$$

Se tiene

$$k \subseteq L \subseteq L(\alpha) \quad (\subseteq \Sigma)$$

Puesto que cada a_i es algebraico sobre k , L es extensión finita de k (teorema 3); igualmente, $L(\alpha)$ es extensión finita de L . Luego $L(\alpha)$ es extensión finita

de k , y, por el teorema 1, a es algebraico sobre k .

De los teoremas 1 y 3 resulta que *un supercuerpo $K = k(a_1, \dots, a_n)$ de k obtenido por la adjunción de un número finito de elementos a_i algebraicos sobre k , es una extensión algebraica de k* . Se deduce de aquí el teorema siguiente, más general.

Teorema 6. — *Toda extensión $K = k(A)$ obtenida por la adjunción al cuerpo k de un conjunto A (incluso infinito) de elementos algebraicos sobre k , es una extensión algebraica de k .*

Por la definición dada en el capítulo IV, § 3, conviene considerar a k y A como subconjuntos de un mismo cuerpo Ω y $K = k(A)$ es el más pequeño subcuerpo de Ω que contiene a k y a A . Cualquiera sea la parte finita $F = \{a_1, \dots, a_n\}$ de A , K contiene a la extensión $k(F)$; K contiene por consiguiente la reunión $\rho = \bigcup_{F \in \Phi} k(F)$, donde Φ designa la familia de las partes finitas de A . ρ es el conjunto de las expresiones racionales, con coeficientes en k , formadas con los elementos de A , luego ρ es un subcuerpo de Ω que contiene a k y a A , de donde

$$K = \rho.$$

Siendo así, si x es un elemento cualquiera de K , existe una parte finita $F = \{a_1, \dots, a_n\}$ de A tal que $k(F)$ comprende a x como elemento; x es pues, como se ha visto más arriba, algebraico sobre k , y finalmente K es, en efecto, una extensión algebraica de k .

§ 4. Ecuaciones algebraicas

Como se ha demostrado antes (cap. IV, § 7) para que algún polinomio de grado n

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

con coeficientes a_i en un anillo conmutativo A con elemento unidad e , admita por cero un elemento a de A , es necesario y suficiente que sea divisible por $x - a$.

$$f(x) = (x - a)f_1(x), f_1(x) \in A[x], \text{ grado de } f_1 = n - 1.$$

Este resultado podría haberse demostrado calculando

$$f(x) - f(a) = \sum_{i=1}^n a_i(x^i - a^i) = \rho(x)(x - a)$$

con

$$\rho(x) = \sum_{i=1}^n a_i(x^{i-1} + \dots + \alpha^{i-1}).$$

Este cálculo es válido aunque el polinomio $f(x)$ tenga coeficientes de un anillo o un cuerpo no conmutativo; se tiene pues el resultado general: si α es raíz del polinomio $f(x)$, $f(x)$ es divisible a la derecha por $(x - \alpha)$.

Si A es un dominio de integridad (en particular si A es un cuerpo conmutativo), resulta que f tiene en A a lo más n ceros distintos. En efecto, si β es un cero de f distinto de α , se tiene

$$0 = f(\beta) = (\beta - \alpha)f_1(\beta),$$

de donde $f_1(\beta) = 0$ puesto que $\beta - \alpha \neq 0$, luego

$$f_1(x) = (x - \beta)f_2(x), \quad f_2(x) \in A[x], \text{ grado de } f_2 = n - 2,$$

y

$$f(x) = (x - \alpha)(x - \beta)f_2(x), \text{ etc...}$$

A los ceros distintos de f en A corresponden otros tantos factores lineales en una misma descomposición de f : el número de estos ceros no puede exceder al grado de f .

Este resultado es válido aunque el dominio de integridad A no tenga elemento unidad: es suficiente reemplazar A por su cuerpo de fracciones K ; f tiene a lo más n ceros en K , luego también, *a fortiori*, en A .

Pero este mismo resultado no conserva su validez en los anillos con divisores de cero: sobre el anillo $A = \mathbb{Z}/(4)$ de las clases residuales de enteros módulo 4, por ejemplo el polinomio $2x \in A[x]$, de primer grado, tiene dos ceros distintos: $\alpha = 0, \beta = 2$ (0, 2 significan aquí las clases módulo 4). Se notará que se trata ahora de un anillo que no es factorial:

$$2x = 2(x - 2)$$

El resultado no subsiste tampoco para los anillos $K[x]$ en los que K sea un cuerpo oblicuo (esto es, no conmutativo). Veamos ahora algunas propiedades para tal anillo de polinomios.

Teorema 1. — Si $(x - \alpha)$ divide a la izquierda al producto $f(x)g(x)$ pero no divide a $f(x)$, se puede encontrar en $K^* = K - \{0\}$ un elemento r tal que $rg(x)r^{-1}$ sea divisible a la izquierda por $(x - \alpha)$.

La identidad de la división a la izquierda de $f(x)$ por $(x - a)$ se escribe

$$f(x) = (x - a) h(x) + r$$

con $0 \leq r$, grado de $r < \text{grado de } (x - a)$, r es pues un elemento no nulo de K . Por otra parte se tiene por hipótesis

$$f(x) g(x) = (x - a) q(x)$$

Se tiene pues

$$\begin{aligned} r g(x) r^{-1} &= f(x) g(x) r^{-1} - (x - a) h(x) g(x) r^{-1} \\ &= (x - a) q(x) r^{-1} - (x - a) h(x) g(x) r^{-1} = (x - a) l(x). \end{aligned}$$

como queríamos demostrar.

Consideremos entonces el conjunto de los polinomios $g_i(x)$ tales que $ag_i a^{-1}$ sea divisible a la izquierda por el polinomio $\delta(x)$ de $K[x]$ de grado positivo cualquiera que sea el elemento a de K^* . Se verifica inmediatamente que este conjunto es un ideal a la derecha. Tal ideal admite un generador $g_0(x)$ de grado positivo en el que se puede tomar el coeficiente director igual a 1.

Además, cualquiera que sea $\lambda \in K^*$ el polinomio $\lambda g_0 \lambda^{-1}$ pertenece a este ideal y, teniendo el mismo grado que g_0 y el mismo coeficiente director, coincide con $g_0(x)$. Todo coeficiente a_i de g_0 es pues tal, que

$$\lambda a_i \lambda^{-1} = a_i \quad \forall \lambda \in K^* ;$$

$g_0(x)$ es por esto un polinomio de $\Omega[x]$, donde Ω es el centro del cuerpo K . Se tiene así:

Teorema 2. — Si el polinomio $g(x)$ es tal, que existe un polinomio de grado positivo divisor a la izquierda de $ag(x)a^{-1}$, $\forall a \in K^*$, $g(x)$ admite un divisor a la izquierda y a la derecha de grado positivo cuyos coeficientes pertenecen al centro Ω de K .

Vamos a dar ahora un teorema importante relativo a las ecuaciones que tienen sus coeficientes en el centro Ω del cuerpo oblicuo K . Notemos primero que si $f(x)$ y $h(x)$ son dos polinomios de $K[x]$ cuyo producto $f(x) h(x)$ es un polinomio de $\Omega[x]$, se tiene:

$$f(x) h(x) = h(x) f(x).$$

Esto resulta inmediatamente de que $g(x) = f(x)h(x)$ es permutable con todo polinomio $l(x)$ de $K[x]$. Tomando como $l(x)$ el polinomio $h(x)$, resulta

$$h(x)(f(x)h(x)) = (f(x)h(x))h(x).$$

Pero en virtud de la asociatividad, el primer miembro se puede escribir $(h(x)f(x))h(x)$ y la regla de simplificación implica la relación a demostrar. Resulta de esto que si c es raíz de $g(x) \in \Omega[x]$, $x - c$ divide también a $g(x)$ por la izquierda.

Teorema 3. — Si $g(x)$ es un polinomio irreducible en el anillo $\Omega[x]$, donde Ω es el centro del cuerpo oblicuo K , y si c es una raíz de $g(x)$ en K , cualquiera sea $t \in K^* = K - \{0\}$, tct^{-1} es raíz de $g(x) = 0$, y toda raíz c' de $g(x) = 0$ en K^* es de la forma $c' = tct^{-1}$.

Se tiene primero:

$$tg(x)t^{-1} = \sum_{i=0}^n ta_i x^i t^{-1} = \sum_{i=0}^n a_i t x^i t^{-1} = \sum_{i=0}^n a_i (txt^{-1})^i,$$

y esto demuestra, que si $g(c) = 0$, también

$$tg(c)t^{-1} = 0 = g(txt^{-1}).$$

Sea ahora c' otra raíz de $g(x) = 0$. Se tiene:

$$tg(x)t^{-1} = g(x) = (x - c')h(x) = (x - tc't^{-1})(th(x)t^{-1})$$

para cualquier elemento t no nulo de K . Si se puede encontrar $t^* \in K^*$ tal que $t^*h(x)t^{*-1}$ no sea divisible a la izquierda por $(x - c)$ el teorema 1 nos permite concluir que existe $r \in K^*$ tal que $r(x - t^*c't^{*-1})r^{-1} = x - rt^*c't^{*-1}r^{-1}$ sea divisible por $(x - c)$ lo que exige $c = rt^*c't^{*-1}r^{-1}$, que es el resultado buscado con $t = (rt^*)^{-1}$. Ahora bien, si $(x - c)$ dividiera a la izquierda a $th(x)t^{-1}$ para todo elemento t no nulo de K , $h(x)$ admitiría, según el teorema 2, un divisor a izquierda y derecha que pertenecería a $\Omega[x]$. Pero este divisor dividiría a $g(x)$, que en consecuencia no sería irreducible en $\Omega[x]$.

Se puede aún, para dos polinomios $f(x)$, $g(x)$ de $K[x]$, definir un m.c.d., de coeficiente director 1, a la izquierda por ejemplo, considerando el ideal a la de-

recha de los polinomios de la forma $fu + gv$ ($u, v \in K[x]$). Se tiene para este m.c.d., que indicaremos por d_g ,

$$d_g = fu' + vg', \quad f = d_g f', \quad g = d_g g'.$$

Si en un supercuerpo de K , f y g tienen un cero común a , $x - a$ divide a la izquierda a f y a g , por consiguiente a d_g , y d_g no será una constante.

Si se supone f irreducible y de coeficiente director igual al elemento unidad, se tiene $f = d_g$ y f divide a g a la izquierda. Se puede entonces enunciar:

Lema. — Si un polinomio irreducible $f(x)$ de $K[x]$ admite en un supercuerpo K' de K un cero común a con un polinomio $g(x) \in K[x]$, $f(x)$ divide a $g(x)$.

Sentado esto, dado un polinomio $f(x) \in K[x]$, irreducible o no, sobre un cuerpo conmutativo K , propongámonos definir y estudiar el orden de multiplicidad de una raíz a de la ecuación algebraica

$$(1) \quad f(x) = 0, \quad f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$$

perteneciendo esta raíz a a un supercuerpo K' de K .

Diremos que a es raíz o cero de orden μ para la ecuación (1) (o cero de orden μ para el polinomio f) si se tiene

$$f(x) = (x - a)^\mu q(x), \quad q(x) \in K'[x]$$

$$q(a) \neq 0;$$

(si $\mu = 1$, la raíz a se llama simple; si $\mu = 2$, doble; si $\mu > 1$, múltiple); el entero positivo μ se llama orden de multiplicidad del cero a , o de la raíz a .

Como en álgebra elemental, conviene introducir la derivada del polinomio $f(x)$, pero aquí por vía puramente algebraica.

Para expresar bajo qué condición el entero $\mu > 0$, definido por

$$f(x) = (x - a)^\mu q(x) \quad \text{con} \quad q(a) \neq 0$$

es superior a 1, escribamos, puesto que $f(a) = 0$,

$$f(x) = f(x) - f(a)$$

y, designando por y una nueva indeterminada, consideremos en el anillo $K[x, y]$

el polinomio

$$f(x) - f(y) = \sum_{k=1}^n a_k(x^k - y^k) = (x - y)\Phi(x, y)$$

donde

$$\Phi(x, y) = \sum_{k=1}^n a_k(x^{k-1} + x^{k-2}y + \dots + y^{k-1})$$

Se tiene inmediatamente

$$(x - a)^{\mu-1}q(x) = \Phi(x, a) \in K'[x].$$

La desigualdad $\mu > 1$ implica $\Phi(a, a) = 0$ e inversamente si el polinomio $\Phi(x, a) \in K'[x]$ se anula para $x = a$, es divisible por $x - a$, lo que exige $\mu > 1$ puesto que $q(a) \neq 0$. La condición necesaria y suficiente buscada es pues

$$(2) \quad \Phi(a, a) = 0$$

Pero el primer miembro es también el valor para $x = a$ del polinomio obtenido tomando $y = x$ en $\Phi(x, y)$:

$$\varphi(x) = \Phi(x, x) = \sum_{k=1}^n k a_k x^{k-1} = a_1 + 2a_2x + \dots + na_nx^{n-1}$$

polinomio de $K[x]$ que se llama *derivada de $f(x)$* y se designa por $f'(x)$.

Finalmente, para que a sea un cero múltiple de f ($\mu > 1$), es necesario y suficiente que sea también cero de la derivada de f :

$$(3) \quad f'(a) = 0$$

Propiedades de la derivada. — 1) La derivada

$$f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1} \quad (a_n \neq 0)$$

del polinomio de grado n

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

es a lo más de grado $n - 1$. Es efectivamente de grado $n - 1$ si el cuerpo K es de característica 0; si la característica de K es p , el grado de $f'(x)$ resulta infe-

rior a $n - 1$ siempre que el grado n de $f(x)$ sea múltiplo de la característica.

2) La suma $s = f + g$ de dos polinomios tiene por derivada la suma $f' + g' = s'$ de las derivadas de f y g :

$$(f + g)' = f' + g'$$

En efecto, si se pone $g(x) - g(y) = (x - y) \Gamma(x, y)$,

$$\begin{aligned} s(x) - s(y) &= f(x) - f(y) + g(x) - g(y) \\ &= (x - y) [\Phi(x, y) + \Gamma(x, y)] \end{aligned}$$

de donde

$$s'(x) = \Phi(x, x) + \Gamma(x, x) = f'(x) + g'(x).$$

3) El producto $p = fg$ de los polinomios $f(x)$, $g(x)$ tiene por derivada $fg' + f'g$. En efecto,

$$\begin{aligned} p(x) - p(y) &= f(x)g(x) - f(y)g(y) \\ &= f(x)[g(x) - g(y)] + g(y)[f(x) - f(y)] \\ &= (x - y) \{ f(x) \Gamma(x, y) + g(y) \Phi(x, y) \} \end{aligned}$$

de donde

$$p'(x) = f(x)\Gamma(x, x) + g(x)\Phi(x, x)$$

es decir

$$p'(x) = f(x)g'(x) + g(x)f'(x)$$

o, también,

$$(fg)' = fg' + f'g$$

De esta se deduce por recurrencia la fórmula de Leibnitz

$$(f_1 f_2 \dots f_r)' = \sum_{i=1}^r f_1 \dots f_{i-1} f'_i f_{i+1} \dots f_r$$

y

$$(f^r)' = r f^{r-1} f'$$

Para un cuerpo K de característica p , $p \neq 0$, la derivada de f^r cuando r es múltiplo de p es el polinomio nulo:

$$(f^{\lambda p})' = 0 \quad \text{en particular} \quad (x^{\lambda p})' = 0$$

y todo polinomio en x^p

$$h(x) = c_0 + c_1 x^p + \dots + c_\lambda x^{\lambda p} \in K[x^p]$$

tiene, asimismo, derivada nula:

$$h'(x) = 0.$$

Recíprocamente, si un polinomio

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in K(x)$$

de grado $n \geq 1$ ($a_n \neq 0$) tiene derivada nula, esto exige que K sea de característica $p \neq 0$ y, además, que se tenga

$$\lambda a_\lambda = 0 \quad (\lambda = 1, \dots, n)$$

de donde, para los valores de λ que no son múltiplos de p :

$$a_\lambda = 0 \quad (\lambda \not\equiv 0 \pmod{p})$$

luego $f(x)$ es un polinomio en x de la forma (4): $f(x) \in K[x^p]$

En resumen:

Para característica cero, la derivada de un polinomio $f(x) = a_0 + \dots + a_n x^n$ de grado $n \geq 1$ ($a_n \neq 0$) no es nunca nula. Para característica $p \neq 0$ los polinomios de grado $n \geq 1$ que tienen derivada nula son los polinomios en x^p

$$(4) \quad h(x) = c_0 + c_1 x^p + \dots + c_\lambda x^{\lambda p} \quad (\lambda \geq 1, c_\lambda \neq 0, n = \lambda p).$$

Estamos ahora en disposición de tratar la cuestión siguiente:

¿Puede tener raíces múltiples un polinomio irreducible $f(x) \in K[x]$?

Si α , elemento de un supercuerpo de K , es raíz múltiple para $f(x)$ se tendrá $f(\alpha) = 0$, $f'(\alpha) = 0$. Puesto que $f(x)$ es irreducible por hipótesis, deberá dividir a $f'(x)$, según un lema anterior:

$$f'(x) = f(x)q(x), \quad q(x) \in K[x].$$

Por ser $K[x]$ un dominio de integridad el producto de dos polinomios tiene por grado la suma de los grados de ambos. Como el grado de f' es inferior al de f , la igualdad anterior exige $q = 0$, $f' = 0$, y por consiguiente $p \neq 0$, (como siempre, p indica la característica del cuerpo K). Así:

Teorema 4. — *Solamente para un campo K de característica $p \neq 0$, puede ocurrir que un polinomio $f(x)$ irreducible sobre K tenga raíces múltiples. Para que sea así es necesario y suficiente que $f(x)$ tenga una derivada nula, o también, que sea un polinomio en x^p .*

Queda todavía, desde luego, estudiar si esta condición necesaria y suficiente es compatible con la irreducibilidad del polinomio $f(x)$. Por lo pronto, introduciremos las siguientes definiciones:

Un polinomio irreducible $f(x) \in K[x]$ de grado $n \geq 1$ se llama *separable* si sólo tiene raíces simples, *inseparable* en caso contrario ¹.

Si todo polinomio irreducible (de grado $n \geq 1$) es separable en $K[x]$, el cuerpo K se llama *perfecto*. Todo cuerpo de característica nula es perfecto.

Un *elemento algebraico* sobre K cuyo polinomio característico $f(x) \in K[x]$ es separable, también se llama *separable*. Según el lema, cualquier polinomio irreducible sobre K del que a sea un cero no difiere del polinomio característico de a más que por un factor constante, luego tiene las mismas raíces. Se puede pues decir: Un elemento algebraico sobre K es separable si es raíz de un polinomio irreducible sobre K que no tiene más que raíces simples.

Una *extensión algebraica* Σ de K se llama separable si todo elemento de Σ es separable sobre K . Según las mismas definiciones, *toda extensión algebraica de un cuerpo perfecto es separable*.

Se llama cuerpo *algebraicamente cerrado* un cuerpo Ω tal, que todo polinomio del anillo $\Omega[x]$ se descompone totalmente en este anillo en factores lineales (ejemplo: el cuerpo de los números complejos, según el teorema de d'Alembert). Un cuerpo tal es *perfecto*, puesto que los únicos polinomios irreducibles de $\Omega[x]$ son de primer grado.

Los dos teoremas siguientes expresan una *condición necesaria y suficiente para que un cuerpo K de característica $p (\neq 0)$ sea perfecto*; deduciremos un nuevo tipo importante de cuerpo perfecto y un ejemplo sencillo de cuerpo imperfecto.

Teorema 5 a (condición suficiente). — *Si todo elemento c de un cuerpo K de característica $p (\neq 0)$ admite en K una raíz a de índice p , ($a^p = c$) K es un cuerpo perfecto.*

Bastará demostrar que un polinomio que tenga su derivada nula, por ende de la forma

$$h(x) = c_0 + c_1 x^p + \dots + c_\lambda x^{\lambda p}, \quad c_i \in K$$

¹ Es conveniente decir que un polinomio $f(x) \in K[x]$ es separable si todos sus factores irreducibles son separables.

no es irreducible sobre K .

Existe en K algún a_i tal que $c_i = a_i^p$, luego

$$h(x) = a_0^p + a_1^p x^p + \dots + a_\lambda^p x^{\lambda p} = [g(x)]^p$$

donde $g(x) = a_0 + a_1 x + \dots + a_\lambda x^\lambda \in K[x]$. Un tal polinomio, $h(x)$, *no es irreducible*. Luego todo polinomio *irreducible* sobre K tiene una derivada diferente de cero, por consiguiente es separable y K es perfecto.

Aplicación. — Observemos en primer lugar, que si en un cuerpo K de característica $p \neq 0$, un elemento c tiene una raíz a de índice p , esta raíz es única. La igualdad $a^p = b^p$ se escribe en efecto

$$a^p - b^p = (a - b)^p = 0 \quad \text{lo que implica} \quad a = b.$$

Si entonces K *no tiene más que un número finito de elementos*, el conjunto de potencias p -ésimas $\{x^p; x \in K\}$ coincide necesariamente con K , puesto que la aplicación $x \rightarrow x^p$ de K en sí mismo es, según lo que precede, inyectiva, y puesto que K es finito, exhaustiva y *biyectiva*. Resulta de ello que K es perfecto, según el teorema 5 a.

Recordemos (cap. IV, § 3) que un cuerpo conmutativo K con un número finito de elementos es un *campo de Galois* (o cuerpo de Galois). Su característica p es ciertamente distinta de cero (todo cuerpo de característica nula tiene un subcuerpo primo isomorfo al cuerpo de los racionales, luego es infinito).

Así: *todo campo de Galois es un cuerpo perfecto*.

Teorema 5 b (condición necesaria). — Si existe en un cuerpo Λ de característica $p \neq 0$ un elemento c que no posee, en Λ , raíz de índice p , Λ es *imperfecto*.

Consideremos el polinomio

$$h(x) = x^p - c \in \Lambda[x]$$

y sea $f(x)$ un factor *irreducible* de $h(x)$ en $\Lambda[x]$.

El grado de f es mayor que 1, pues un factor lineal $x - \theta \in \Lambda[x]$ daría una raíz p -ésima de c , θ , en Λ .

Sea $\Lambda(\alpha)$ un cuerpo de ruptura de f ; α verifica, en $\Lambda(\alpha)$, la igualdad $f(\alpha) = 0$, luego $h(\alpha) = 0$, es decir

$$\alpha^p = c$$

de donde

$$h(x) = x^p - c = x^p - \alpha^p = (x - \alpha)^p$$

lo que implica, por la factorización única de h en $\Lambda(a)[x]$,

$$f(x) = (x - a)^r \quad \text{con } 1 < r \leq p$$

$f(x)$ irreducible sobre Λ y admitiendo la raíz a múltiple de orden $r > 1$, es inseparable sobre Λ , Λ es imperfecto.

Pero además $f(x)$ tiene una derivada nula cuyo grado es múltiplo de p , lo que exige $r = p$ y $f(x) = (x - a)^p = h(x)$. Luego:

Si un elemento c de Λ , cuerpo de característica $p \neq 0$, no tiene raíz p -ésima en Λ , $x^p - c$ es un polinomio irreducible sobre Λ , e inseparable. Este polinomio se descompone completamente sobre su cuerpo de ruptura, tomando la forma $(x - a)^p$.

Ejemplo. — Designemos por $k(= \mathbf{Z}/(p))$ el cuerpo de las clases de restos de enteros módulo p , y tomemos $\Lambda = k(t)$ donde t es una indeterminada (Λ es entonces una *extensión transcendente simple* del cuerpo primo de característica p).

El elemento $\alpha = \sqrt[p]{t}$ es algebraico sobre Λ y no pertenece a Λ (como tampoco α^m para $m = 1, 2, \dots, p - 1$).

En efecto, $\alpha^m \in \Lambda$, es decir

$$\alpha^m = \frac{a_0 t^r + \dots + a_r}{b_0 t^s + \dots + b_s} \quad (a_i, b_i \in k, r \geq 0, s \geq 0, a_0 \neq 0, b_0 \neq 0,$$

implicaría, elevando a la potencia p ,

$$t^m (b_0 t^s + \dots + b_s)^p = (a_0 t^r + \dots + a_r)^p$$

lo que exigiría

$$m + ps = pr$$

igualdad imposible para $m = 1, 2, \dots, p - 1$.

§ 5. Enteros algebraicos

Sea A un subanillo de un anillo conmutativo B ; suponemos que A posee elemento unidad e .

Definición. — Se dice que un elemento ξ de B es *entero algebraico* sobre A si verifica una ecuación de la forma

$$(1) \quad x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad a_i \in A,$$

en la cual el coeficiente director es igual al elemento unidad e .

Ejemplo. — Según el teorema 4 (§ 3), los números algebraicos es decir los números complejos que son algebraicos sobre el cuerpo $\mathbb{Q}$ de los racionales, forman un cuerpo $\mathbb{L}$,

$$\mathbb{Q} \subset \mathbb{L} \subset \mathbb{C}.$$

La definición precedente conduce a distinguir entre los elementos de $\mathbb{L}$ ($= B$) los que son enteros algebraicos sobre el anillo $\mathbb{Z}$ ($= A$) de enteros: estos números son llamados generalmente *enteros algebraicos* (sin más). Por ejemplo, $\sqrt{2}$, $\frac{-1 + \sqrt{5}}{2}$, que verifican respectivamente las ecuaciones

$$x^2 - 2 = 0, \quad x^2 + x - 1 = 0$$

son enteros algebraicos.

Observación. — Si el anillo A es factorial, admite, como dominio de integridad, un cuerpo de cocientes K . Todo elemento ξ de un supercuerpo Σ de K que es entero algebraico sobre A , es algebraico sobre K . Si el primer miembro de la ecuación (1) verificada por ξ se descompone en $K[x]$:

$$x^n + a_1x^{n-1} + \dots + a_n = f_1(x) \dots f_r(x), \quad f_i(x) \in K[x],$$

y si $f_i^*(x)$ es el polinomio primitivo del anillo $A[x]$ procedente del factor $f_i(x)$, $f_i^*(x) = \lambda_i f_i(x)$, $\lambda_i \in K$, se puede escribir la ecuación (1) en la forma

$$c(x^n + a_1x^{n-1} + \dots + a_n) = f_1^*(x) \dots f_r^*(x), \quad c \in K;$$

esta igualdad implica $c \in A$ y además el primer miembro, producto de polinomios primitivos, es primitivo (cap. IV, § 6, lema 2), c es entonces una unidad de A y lo mismo sucede con cada uno de los coeficientes directores de los polinomios $f_i^*(x)$. Ahora bien, ξ anula al menos uno de estos polinomios. Finalmente, vemos que ξ verifica una ecuación algebraica *irreducible* sobre K cuyo primer miembro es un polinomio de $A[x]$ con su coeficiente director igual a e .

Para todo elemento β del anillo B , el conjunto $A[\beta]$ de expresiones polinómicas en β con coeficientes en A es, no solamente un subanillo de B , sino un A -módulo (submódulo de B que es, él mismo, un A -módulo). Si ξ es un entero alge-

braico sobre A , $A[\xi]$ es el *módulo de tipo finito*

$$\sum_{i=0}^{n-1} A\xi^i = (e, \xi, \dots, \xi^{n-1})$$

engendrado por los n elementos $e = \xi^0, \xi, \dots, \xi^{n-1}$; la ecuación (1) implica en efecto $\xi^n \in (e, \xi, \dots, \xi^{n-1})$ y de ello resulta inmediatamente, por recurrencia sobre el exponente h , que, para todo número natural $h(\geq n)$, $\xi^h \in (e, \xi, \dots, \xi^{n-1})$.

Luego, $A[\xi]$ está contenido en un subanillo B' de B que es un A -módulo de tipo finito (basta tomar $B' = (e, \xi, \dots, \xi^{n-1})$).

Para un elemento ξ de B , esta última propiedad implica a su vez que *existe en B un A -módulo M de tipo finito tal que se tenga*

$$\begin{array}{ll} 1^\circ & \xi M \subseteq M, \\ 2^\circ & A[\xi] \cap (0 : M) = (0) \end{array}$$

designando $0 : M$ el conjunto de elementos β de B tales que $\beta M = (0)$; la condición 2° significa pues que 0 es el único elemento η de $A[\xi]$ tal que $\eta m = 0$ para todo $m \in M$. Estas condiciones quedan verificadas si se toma $M = B'$:

1° puesto que $\xi M \subseteq B'^2 \subseteq B' = M$,

2° puesto que el elemento unidad e pertenece a M y $\eta e = 0$ da $\eta = 0$.

Por último probemos que, *para un elemento ξ de B , la existencia de un A -módulo M de tipo finito contenido en B y cumpliendo las propiedades 1° y 2° implica que ξ es entero algebraico sobre A .*

Sea $(m_1, \dots, m_n)$ un sistema de generadores del A -módulo M :

$$M = \sum_{i=1}^n A m_i.$$

Según 1° , tenemos $\xi M \subseteq M$, luego

$$\xi m_\lambda = \sum_{\mu=1}^n a_{\lambda\mu} m_\mu \quad (\lambda = 1, \dots, n; a_{\lambda\mu} \in A).$$

Designando por $\delta_{\lambda\mu}$ los símbolos de Kronecker, pongamos

$$c_{\lambda\mu} = \delta_{\lambda\mu} \xi - a_{\lambda\mu} \in A[\xi];$$

las ecuaciones (2) se escriben

$$\sum_{\mu=1}^n c_{\lambda\mu} m_{\mu} = 0 \quad (\lambda = 1, \dots, n).$$

Sea entonces $C_{\mu\lambda}$ el menor (tomado con su signo exterior) de $c_{\lambda\mu}$ en el determinante $D = |c_{\lambda\mu}|$; las ecuaciones (2') implican, para todo índice r ($1 \leq r \leq n$):

$$0 = \sum_{\lambda=1}^n C_{r\lambda} \sum_{\mu=1}^n c_{\lambda\mu} m_{\mu} = \sum_{\mu=1}^n \left(\sum_{\lambda=1}^n C_{r\lambda} c_{\lambda\mu} \right) m_{\mu};$$

teniendo en cuenta las identidades fundamentales

$$\sum_{\lambda=1}^n C_{r\lambda} c_{\lambda\mu} = \delta_{r\mu} D,$$

resulta

$$D m_r = 0 \quad (r = 1, \dots, n),$$

luego $D \in 0 : M$. Como $D = |\delta_{\lambda\mu} \xi - a_{\lambda\mu}| \in A[\xi]$, resulta, según 2.º, $D = 0$, lo que constituye una ecuación algebraica en ξ , de grado n , con coeficientes en A y cuyo coeficiente director es igual a e .

Finalmente, podemos enunciar el teorema que sigue.

Teorema 1. — *Para que un elemento ξ de B sea entero algebraico sobre el subanillo A de B (que contiene el elemento unidad e), es necesario y suficiente que verifique una cualquiera de las tres condiciones:*

- a) *el anillo $A[\xi]$ es un A -módulo de tipo finito;*
- b) *$A[\xi]$ está contenido en un subanillo B' de B que es un A -módulo de tipo finito;*
- c) *existe en B un A -módulo M de tipo finito tal que se tenga:*

$$\xi M \subseteq M,$$

y

$$A[\xi] \cap (0 : M) = (0).$$

Lema. — *Si los elementos $\xi_1, \dots, \xi_n$ de B son enteros algebraicos sobre A , el anillo $A[\xi_1, \dots, \xi_n]$ es un A -módulo de tipo finito.*

Según la condición α del teorema 1, el lema es cierto para $n = 1$. Razonemos por recurrencia sobre n , suponiendo que el anillo

$$A' = A[\xi_1, \dots, \xi_{n-1}]$$

es un A -módulo de tipo finito:

$$A' = \sum_{j=1}^k A \varphi_j, \quad (\varphi_j \in A').$$

El elemento ξ_n , entero algebraico sobre A , es entero algebraico sobre A' , por consiguiente

$$A'' = A'[\xi_n] = A[\xi_1, \dots, \xi_{n-1}, \xi_n]$$

es un A' -módulo de tipo finito:

$$A'' = \sum_{i=1}^h A' u_i \quad (u_i \in A''),$$

de donde

$$A'' = \sum_{i=1}^h \sum_{j=1}^k A u_i \varphi_j$$

y A'' es un A -módulo de tipo finito.

Teorema 2. — 1.º El conjunto $\bar{A}$ de elementos del anillo B que son enteros algebraicos sobre A es un anillo (que contiene a A):

2.º Todo elemento ξ de B o de un superanillo de B que verifique una ecuación de la forma

$$x^n + b_1 x^{n-1} + \dots + b_n = 0,$$

donde las b_i pertenecen a B y son enteros algebraicos sobre A , es entero algebraico sobre A .

1.º Sean ξ, η dos elementos de B enteros algebraicos sobre A . Según el lema precedente, el anillo $A[\xi, \eta]$ es un A -módulo de tipo finito; $\xi - \eta$ y $\xi\eta$, pertenecen a este módulo y son enteros algebraicos sobre A (según la condición b del teorema 1).

2.º El anillo $A[b_1, \dots, b_n] = R$ es, según el lema, un A -módulo de tipo finito; siendo ξ entero algebraico sobre R , el anillo $R[\xi]$ es un R -módulo de tipo finito.

Resulta de ello (como en la demostración del lema) que $R[\xi]$ es un A -módulo de tipo finito; ξ es pues entero algebraico sobre A .

§ 6. Raíces de la unidad

Sea e el elemento unidad del cuerpo primo Π , que será de característica 0 o p . Consideremos el polinomio $f(x) = x^m - e$ y la ecuación

$$(1) \quad x^m - e = 0$$

Sea Δ el cuerpo de descomposición de $f(x)$; Δ se obtiene a partir de Π por un número finito de adjunciones simbólicas, y todo cuerpo obtenido a partir de un cuerpo conmutativo por adjunción simbólica es conmutativo: Δ es pues conmutativo.

Las raíces de (1) en Δ son, por definición, las *raíces m -ésimas de la unidad sobre Π* . Forman un grupo multiplicativo (abeliano) puesto que

$$\xi^m = e = \eta^m \quad \text{implica} \quad (\xi/\eta)^m = e.$$

En este grupo Γ , el orden de un elemento cualquiera ξ divide a m . El cuerpo Δ se llama también *cuerpo de las raíces m -ésimas de la unidad, sobre Π* .

Supongamos que m no es múltiplo de la característica (hipótesis que se cumple desde luego en el caso de característica 0). Entonces

$$f'(x) = mx^{m-1} \neq 0$$

y 0, única raíz de la derivada, no es solución de la ecuación (1); ésta no tiene pues más que raíces simples y el número de raíces m -ésimas de la unidad distintas es exactamente m (en Δ).

Observación. — Si por el contrario $m = \lambda p$, $p \neq 0$, se tiene

$$x^m - e = x^{\lambda p} - e^p = (x^\lambda - e)^p$$

Las raíces m -ésimas no son otras que las raíces λ -ésimas; hay a lo más λ distintas (si λ es también múltiplo de p , la reducción se repite).

Teorema. — *El grupo multiplicativo Γ de las raíces m -ésimas de la unidad (para m no múltiplo de la característica) es cíclico.*

Observemos en primer lugar que, si la característica es nula, el cuerpo de descomposición puede considerarse como subcuerpo del cuerpo de los números

complejos (siendo Π el de los racionales); las raíces de (1) son

$$\zeta_k = \cos \frac{2k\pi}{m} + i \operatorname{sen} \frac{2k\pi}{m} = \zeta_1^k \quad (k = 0, 1, 2, \dots, m-1)$$

Forman efectivamente un grupo cíclico Γ .

Demos una demostración válida cualquiera que sea la característica.

Si Γ es de orden m , descompongamos m en factores primos

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

m/p_i no es múltiplo de la característica p , por lo que la ecuación $x^{m/p_i} = e$, tiene m/p_i raíces distintas en Δ ; puesto que Γ tiene m elementos distintos, podemos encontrar en Γ un elemento a_i distinto de las raíces en cuestión: $a_i^{m/p_i} \neq e$. Entonces sea

$$c_i = a_i^{m/p_i^{\alpha_i}} \in \Gamma;$$

tenemos

$$c_i^{p_i^{\alpha_i}} = a_i^m = e$$

luego el orden de c_i divide a $p_i^{\alpha_i}$, luego es una potencia de p_i . Además,

$$c_i^{p_i^{\alpha_i-1}} = a_i^{m/p_i} \neq e,$$

luego el orden de c_i es *exactamente* $p_i^{\alpha_i}$.

El elemento $\zeta = c_1 \dots c_k$ es, según un teorema elemental (cap. VIII, § 4, ejemplo 4), de orden $p_1^{\alpha_1} \dots p_k^{\alpha_k} = m$.

El elemento ζ es pues un generador de Γ , y Γ es cíclico. Se dice que ζ es una *raíz primitiva* de la ecuación (1); las m raíces $\zeta_1, \dots, \zeta_m$ de (1) son potencias de ζ y tenemos

$$\Delta = \Pi(\zeta_1, \dots, \zeta_m) = \Pi(\zeta)$$

Δ es pues una extensión algebraica simple de Π .

§ 7. Campos de Galois

Sea K un campo de Galois, de característica p . Sea Π su subcuerpo primo y $r = (K : \Pi)$ el grado de K sobre Π , evidentemente *finito* puesto que K es

finito. Sea $(a_1, \dots, a_r)$ una base de K sobre Π : todo elemento a de K tiene una representación única

$$a = \alpha_1 a_1 + \dots + \alpha_r a_r, \quad \alpha_i \in \Pi,$$

y puesto que cada α_i puede tomar p valores distintos, el número N de elementos de K es

$$N = p^r$$

Así, el número N de elementos de un campo de Galois es una potencia de su característica p .

El grupo multiplicativo $K^* = K - \{0\}$ de K es de orden $N - 1$; se tiene entonces para todo $a \in K^*$:

$$a^{N-1} = e$$

y, por consiguiente, para todo $a \in K$

$$a^N = a$$

puesto que esta ecuación es cierta para $a = 0$. Los N elementos de K son pues las raíces de la ecuación

$$x^N - x = 0 \quad \text{donde} \quad x^N - x \in \Pi[x]$$

y estas raíces son simples.

El polinomio $x^N - x$ se descompone en $K[x]$ en factores lineales; K es su cuerpo de descomposición puesto que un cuerpo Σ tal que $\Pi \subset \Sigma \subset K$ tiene menos de N elementos, luego no puede contener los N ceros distintos del polinomio $x^N - x$.

El cuerpo de Galois K está pues determinado a menos de un isomorfismo por su subcuerpo primo Π (o su característica p) y por el número $N = p^r$ de sus elementos, luego finalmente por N , puesto que el conocimiento del número "primario" $N = p^r$ implica el de p .

Probemos que recíprocamente, dados p (primo) y r (número natural), existe un campo de Galois K de orden p^r . Sea Π el cuerpo primo de característica p ; consideremos en el anillo $\Pi[x]$ el polinomio

$$f(x) = x^N - x, \quad \text{donde} \quad N = p^r.$$

Por otra parte, en el anillo euclídeo $k[x]$ todo ideal es *principal*, luego $\mathfrak{a} = (p)$, $p = p(x) \in k[x]$.

Distinguiremos dos casos, según que el ideal $\mathfrak{a}$ sea *nulo o distinto de (0)*.

I. $\mathfrak{a} = (0)$. No existe ningún polinomio no nulo $f(x)$ de $k[x]$ que tome el valor cero para $x = \alpha$. En este caso se dice que α es *trascendente* sobre k y que la extensión simple $k(\alpha)$ es *trascendente*. Entonces se tiene

$$k[x] = k[x]/(0) \simeq k[\alpha]$$

lo que entraña el isomorfismo de los *cuerpos de fracciones*

$$k(x) \simeq k(\alpha),$$

y la extensión simple $k(\alpha)$ es *isomorfa sobre k* con el cuerpo de fracciones racionales $k(x)$.

II. $\mathfrak{a} = (p)$, $p \neq 0$.

El polinomio $p = p(x) \in k[x]$ no es una constante, puesto que en el homomorfismo θ , $f(x) \rightarrow f(\alpha)$ la imagen de una constante es ella misma y aquí se tiene $p(x) \neq 0$, $p(\alpha) = 0$. Así, $p(x)$ es un polinomio de grado ≥ 1 , e incluso de grado ≥ 2 si $k(\alpha) \neq k$, como es natural suponer. En efecto, si $p(x) = ax + b$, $a, b \in k$, de $p(\alpha) = a\alpha + b = 0$ se deduce $\alpha \in k$, $k(\alpha) = k$.

Por ser el ideal $\mathfrak{a} = (p(x))$ *primo* en el anillo euclídeo, y por ende principal, $k[x]$, el polinomio p es *irreducible* sobre k , es decir, irreducible en $k[x]$, será $\mathfrak{a}$ un ideal *maximal* (cap. VII, § 3), y el anillo cociente $k[x]/\mathfrak{a}$ un *cuerpo* (cap. IV, § 8, teor. 1); también será un cuerpo el anillo isomorfo $k[\alpha]$, que por lo tanto coincide con la extensión $k(\alpha)$, y tendremos

$$(1) \quad k(\alpha) = k[\alpha] \simeq k[x]/(p(x)) \quad (\theta)$$

En este caso, la extensión simple $k(\alpha)$ y $k[x]/(p(x))$ son cuerpos *isomorfos sobre k* .

El polinomio $p(x)$ es uno de los generadores del ideal de polinomios $f(x)$ tales que $f(\alpha) = 0$, es decir, uno de los polinomios de *grado mínimo* ν anulados por α . Se le determina completamente haciendo que el coeficiente del término en x^ν sea la unidad: se dice entonces que p es el *polinomio característico* del elemento α . El elemento α se llama *algebraico*, y de grado ν , sobre k . Se dice también que $k(\alpha)$ es una *extensión algebraica simple sobre k* .

La igualdad $k(\alpha) = k[\alpha]$ implica que *todo elemento ξ de la extensión*

Sea K su cuerpo de descomposición, sobre Π ; K contiene los N ceros de f , y éstos son distintos puesto que

$$\begin{aligned} f'(x) &= Nx^{N-1} - e = p^r x^{p^r-1} - e \\ &= -e \neq 0 \quad \forall x \in K. \end{aligned}$$

Pero estos N ceros $\zeta_1, \zeta_2, \dots, \zeta_N (= 0)$ forman ya un cuerpo, puesto que

$$\zeta_i^{p^r} = \zeta_i, \quad \zeta_j^{p^r} = \zeta_j$$

implican

$$(\zeta_i - \zeta_j)^{p^r} = \zeta_i^{p^r} - \zeta_j^{p^r} = \zeta_i - \zeta_j,$$

luego $\zeta_i - \zeta_j$ es un tal cero simultáneamente a ζ_i y ζ_j ; asimismo, para $\zeta_j \neq 0$, el cociente $\zeta_i/\zeta_j (\in K)$ es también un cero de f puesto que

$$\left(\frac{\zeta_i}{\zeta_j}\right)^{p^r} = \frac{\zeta_i^{p^r}}{\zeta_j^{p^r}} = \frac{\zeta_i}{\zeta_j}.$$

El conjunto $\{\zeta_1, \zeta_2, \dots, \zeta_N\} (\subseteq K)$, por ser un cuerpo, es el propio cuerpo de descomposición, y K es de orden $N = p^r$.

Se designa por $CG(p^r)$ o $GF(p^r)$ ¹ el campo de Galois de p^r elementos.

El producto de los elementos no nulos de un campo de Galois es igual a $-e$, puesto que, poniendo $\zeta_N = 0$, se tiene

$$x^{N-1} - 1 = \prod_{i=1}^{N-1} (x - \zeta_i)$$

de donde

$$(2) \quad -1 = \zeta_1 \zeta_2 \dots \zeta_{N-1}$$

(Para $p \neq 2$, p es impar, $N - 1 = p^r - 1$ es par; no es así si $p = 2$, pero entonces $-a = +a \quad \forall a \in K$.)

Observaciones. — 1. Para $r = 1$, $N = p$, $K = \Pi$ es a menos de un isomorfismo el cuerpo de las clases de restos de los enteros módulo p . Para todo elemento x de este cuerpo, se tiene

$$x^p = x$$

¹ Iniciales, obviamente, del "Galois field" inglés. (N. del T.)

luego para todo entero X , se tiene

$$X^p \equiv X \pmod{p} \quad (\text{teorema de Fermat}).$$

2. En el mismo caso particular, (2) da

$$(p-1)! \equiv -1 \pmod{p} \quad (\text{teorema de Wilson}).$$

Teorema 1. — *Todo campo de Galois $K = CG(p^r)$ es extensión algebraica simple de su subcuerpo primo Π .*

El grupo multiplicativo $K^* = K - \{0\}$ de K está formado por las raíces de la ecuación

$$x^{N-1} - e = 0 \quad (N = p^r)$$

es decir por las raíces $(N-1)$ -ésimas de la unidad. Es cíclico

$$K^* = (\zeta)$$

donde ζ es un ζ_i , $\neq e$. Al ser todo $\zeta_j \neq 0$ una potencia de ζ , se tiene

$$K = \Pi(\zeta)$$

Como se ha visto anteriormente, todo campo de Galois es un *cuerpo perfecto*.

Subcuerpos de $K = CG(p^r)$.

Sea K' un subcuerpo de K ; por tanto

$$\Pi \subseteq K' \subseteq K$$

Se tiene

$$r = (K : \Pi) = (K : K') (K' : \Pi)$$

luego el grado $s = (K' : \Pi)$ divide a r . K' es un cuerpo de Galois de orden p^s y sus p^s elementos son los ceros del polinomio

$$g(x) = x^{p^s} - x$$

Observemos, que si β divide a α , $\alpha = \beta\gamma$, se tiene para todo cuerpo (conmutativo) k , en el anillo $k[u]$, la identidad

$$u^\alpha - \epsilon = u^{\beta\gamma} - \epsilon = (u^\beta - \epsilon) [u^{\beta(\gamma-1)} + u^{\beta(\gamma-2)} + \dots + u^\beta + \epsilon]$$

designando ϵ el elemento unidad de k . En particular, puesto que s divide a r :

$$p^r - 1 = (p^s - 1) [p^{r-s} + p^{r-2s} + \dots + p^s + 1]$$

y, puesto que $p^s - 1$ divide a $p^r - 1$:

$$x^{p^r-1} - e = (x^{p^s-1} - e) \cdot F(x), \quad \text{donde} \quad F(x) \in \Pi[x].$$

Resulta de aquí que el polinomio $g(x) = x^{p^s} - x$ divide al polinomio

$$f(x) = x^{p^r} - x;$$

como esta propiedad tiene lugar para todo divisor s de r , y puesto que los ceros de $x^{p^s} - x$ forman un cuerpo, vemos que a todo divisor s de r corresponde un campo de Galois de orden p^s , subcuerpo de $K = CG(p^r)$, formado por 0 y por los elementos de K^* cuyo orden es un divisor de $p^s - 1$. Este subcuerpo es por tanto único.

Además, K es una extensión algebraica simple de K' , $K = K'(c)$, de grado

$$h = \frac{(K : \Pi)}{(K' : \Pi)} = \frac{r}{s};$$

c es un elemento de $K - K'$ que verifica una ecuación irreducible de grado h en $K'[x]$, $g(x) = 0$. Precisemos la forma de esta ecuación; pondremos $p^s = q$, de donde $p^r = q^h$.

Teorema 2. — En $K[x]$, $g[x]$ se descompone completamente en factores lineales, bajo la forma

$$g(x) = (x - c) (x - c^q) \dots (x - c^{q^{h-1}}).$$

Es suficiente demostrar que el segundo miembro $g_1(x)$ es el polinomio característico de c sobre K' ; como es de grado h , tiene el elemento unidad como coeficiente director y tiene con $g(x)$ la raíz común c , probemos para ello que pertenece a $K'[x]$.

Los coeficientes a_i de g_1 son expresiones polinómicas simétricas en $c, c^q, \dots, c^{q^{h-1}}$:

$$a_i = f_i(c, c^q, \dots, c^{q^{h-1}}).$$

Tenemos en particular

$$a_i = f_i(c^q, c^{q^2}, \dots, c^{q^{h-1}}, c) = f_i(c^q, c^{q^2}, \dots, c^{q^{h-1}}, c^q)$$

y, puesto que q es una potencia de la característica, $q = p^s$,

$$f_i(c^q, c^{q^2}, \dots, c^{q^{h-1}}, c^{q^h}) = [f_i(c, c^q, \dots, c^{q^{h-2}}, c^{q^{h-1}})]^q.$$

Cada uno de los coeficientes a_i verifica entonces la ecuación

$$x^q - x = 0$$

y por consiguiente pertenece a K' .

§ 8. Teorema del elemento primitivo

El teorema del elemento primitivo permite constatar, mediante una hipótesis de separabilidad, que una extensión finita (o, si se prefiere, algebraica finita) es una extensión algebraica *simple*.

Teorema. — Si $K = k(\alpha, \beta, \dots, \lambda)$ es una extensión algebraica finita de k y si $\beta, \dots, \lambda$ son separables sobre k , K es una extensión algebraica simple de k :

$$\exists \sigma \in K \quad \text{tal que} \quad k(\sigma) = K.$$

Antes de probar este teorema, observemos que:

- 1.º no es necesario suponer α separable;
- 2.º si la característica es nula, la hipótesis de separabilidad se cumple.

Demostración. — Si k es un campo de Galois, también lo es K , de grado finito sobre k ; K es extensión algebraica simple de su subcuerpo primo Π , $K = \Pi(\zeta)$ (§ 7); como $\Pi \subseteq k \subseteq K$, se tiene también $K = k(\zeta)$.

Supongamos entonces que k tenga una infinidad de elementos distintos, y demostremos en primer lugar el teorema para una extensión de la forma:

$$K = k(\alpha, \beta), \quad \beta \text{ separable.}$$

Sean

$$f(x) = 0 \quad g(x) = 0$$

las ecuaciones irreducibles sobre k verificadas respectivamente por α y β . Sean $\alpha_1, \dots, \alpha_r$ ($\alpha_1 = \alpha$) las raíces de la primera, $\beta_1, \dots, \beta_s$ ($\beta_1 = \beta$) las de la segunda, en un cuerpo de descomposición, Δ , de fg sobre K : por hipótesis, todas las β_j son raíces simples.

Cada una de las ecuaciones en x

$$\alpha_i + x\beta_j = \alpha_1 + x\beta_1 \quad (j \neq 1) \quad \begin{cases} i = 1, \dots, r \\ j = 2, \dots, s \end{cases}$$

tiene una solución en Δ , luego a lo más una solución en k ; siendo k infinito, existe en k un elemento c distinto de todas estas soluciones, luego

$$\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1 \quad \forall i = 1, \dots, r \quad \forall j = 2, \dots, s.$$

Pongamos

$$\sigma = \alpha_1 + c\beta_1 = \alpha + c\beta \in k(\alpha, \beta) \subseteq \Delta$$

Tenemos $k(\sigma) \subseteq k(\alpha, \beta)$; vamos a establecer la igualdad.

Tenemos

$$g(\beta) = 0 \quad \text{y} \quad f(\alpha) = f(\sigma - c\beta) = 0$$

Las ecuaciones en x :

$$\begin{aligned} g(x) &= 0 & g &\in k[x] \subseteq k(\sigma)[x] \subseteq \Delta[x] \\ \varphi(x) &= f(\sigma - cx) & \varphi &\in k(\sigma)[x] \subseteq \Delta[x] \end{aligned}$$

no tienen en Δ , otra raíz común que $\beta = \beta_1$, pues otra raíz β_j de $g = 0$ da a $\sigma - cx$ el valor

$$\sigma - c\beta_j = \alpha_1 + c(\beta_1 - \beta_j) \neq \alpha_i \quad (i = 1, \dots, r)$$

según la elección de c . Luego β es único cero, en $\Delta = k(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$ de

$$\delta(x) = \text{m.c.d. } [g(x), \varphi(x)] \in \Delta[x]$$

(donde δ , que divide a g , se descompone también completamente en factores lineales).

Puesto que β es cero simple de g (según la hipótesis de separabilidad), es también cero simple de $\delta(x)$, que es por consiguiente de primer grado. Puesto que $\delta \in k(\sigma)[x]$, se tiene $\beta \in k(\sigma)$ luego $\alpha = -c\beta + \sigma \in k(\sigma)$, por consiguiente

$$k(\alpha, \beta) \subseteq k(\sigma),$$

de donde se sigue la igualdad

$$k(\alpha, \beta) = k(\sigma).$$

La demostración se termina fácilmente por recurrencia (sobre el número de elementos $\beta, \dots, \lambda$). Supongamos en efecto el teorema cierto para $k(\alpha, \beta, \dots, \lambda)$ y demostrémoslo para $k(\alpha, \beta, \dots, \lambda, \mu)$, siendo μ algebraico y separable sobre k .

Según la hipótesis de recurrencia, existe un elemento

$$\rho \in k(\alpha, \beta, \dots, \lambda) \subseteq k(\alpha, \beta, \dots, \lambda, \mu)$$

tal que

$$k(\alpha, \beta, \dots, \lambda) = k(\rho),$$

de donde

$$k(\alpha, \beta, \dots, \lambda, \mu) = k(\rho, \mu) = K$$

y, según la primera parte de la demostración, existe un elemento σ de K tal que $K = k(\sigma)$ c.q.d.

§ 9. Teorema de Wedderburn

Teorema de Wedderburn. *Todo cuerpo finito es conmutativo.*

Sea σ un cuerpo dado. El centro Ω de σ no es nunca vacío y es al menos de orden 2 puesto que contiene el subcuerpo primo de σ ; sea q su orden.

Demostraremos la propiedad por recurrencia sobre el orden N de σ . La propiedad es cierta para $N=2$, y la suponemos cierta para todo cuerpo de orden estrictamente inferior a N .

El conjunto de los subcuerpos de σ es finito, por lo que hay al menos un subcuerpo de σ maximal γ que contiene a Ω y a un elemento arbitrario s de $\sigma - \Omega$ supuesto no vacío (a menos que se tenga $\sigma = \Omega$ (s), pero entonces σ , extensión simple de un cuerpo conmutativo, es conmutativo). En virtud de la hipótesis de recurrencia, todo subcuerpo maximal es conmutativo. Probemos que hay *un solo* subcuerpo maximal que contiene a s y a Ω ; para ello, probaremos que dos subcuerpos maximales que contienen a Ω , tienen por intersección Ω . Sea $s_1 \in \sigma - \gamma$ y γ_1 un subcuerpo maximal que contiene a Ω y a s_1 . El sistema de generadores $\{\gamma, s_1\}$ engendra a σ puesto que γ es maximal.

Sea $x \in \gamma_1 \cap \gamma$; x es pues permutable con s_1 y con todo elemento de γ , luego con todo elemento del subanillo de σ constituido por las sumas finitas de productos finitos de s_1 con elementos de γ , subanillo que no es otra cosa que el cuerpo σ , puesto que todo subanillo finito de un cuerpo es un cuerpo y puesto que γ , contenido estrictamente en este cuerpo, es maximal en σ ; x es pues un elemento del centro de σ .

Sea q^n el orden de γ ; siendo γ un campo de Galois, se puede obtener por

adjunción simple de un elemento c que verifica en $\Omega[x]$ una ecuación irreducible $g(x) = 0$ que, en $\sigma[x]$, es la ecuación

$$g(x) = (x - c)(x - c^q) \dots (x - c^{q^{n-1}}),$$

y siendo c elemento del cuerpo σ del centro Ω , se sabe que existe $t \in \sigma$ tal que $c^q = tct^{-1}$. Resulta de aquí

$$(c^q)^q = c^{q^2} = tc^qt^{-1} = t^2ct^{-2}$$

y, reiterando:

$$c^{q^h} = tc^{q^{h-1}}t^{-1} = t^hct^{-h}$$

de donde, para todo entero h :

$$t^hc = c^{q^h}t^h.$$

Pero c , elemento de γ , verifica la ecuación $x^{q^n} = x$. Se tiene entonces

$$c^{q^n} = c = t^nc t^{-n}$$

y c , que no era permutable con t , es permutable con t^n . Pero t no pertenece a γ puesto que γ es conmutativo y t no es permutable con c que pertenece a γ ; luego $\{\gamma, t\}$ o incluso $\{\Omega, c, t\}$ es un sistema de generadores para σ , y t^n , que es permutable con todo elemento de este sistema de generadores, es también permutable con todo elemento de σ , luego pertenece a Ω .

Consideremos entonces el subconjunto de σ formado por las sumas finitas

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{ij} c^i t^j, \quad \text{con} \quad c^0 = 1, \quad t^0 = 1 \quad (1 \in \sigma),$$

donde para cada par dado de índices, i, j , se reemplaza a_{ij} por uno de los q elementos de Ω . Se obtienen así q^{n^2} términos todos distintos, pues si no fuera así se deduciría una relación

$$0 = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{ij} c^i t^j = \sum_{j=0}^{n-1} C_j^* t^j,$$

poniendo

$$C_j^* = \sum_{i=0}^{n-1} a_{ij} c^i$$

(con los a_{ij} no todos nulos).

Pero C_j^* es un elemento de γ y c no satisface a ninguna ecuación de grado menor que n en $\Omega[x]$; luego C_j^* no puede ser nulo sin que lo sean todos los a_{ij} de esta relación.

Si se tuviera

$$0 = \sum_{j=0}^{n-1} C_j^* t^j,$$

con los C_j^* no todos nulos, t sería raíz de una ecuación de $\gamma[x]$ de grado $\leq n-1$; sea m el grado mínimo de una ecuación de $\gamma[x]$ satisfecha por t ; se podría escribir:

$$t^m = a_{m-1}t^{m-1} + \dots + a_1t + a_0, \quad m < n.$$

Pero $t^m c = c^{q^m} t^m$; luego se tiene

$$(a_{m-1}t^{m-1} + \dots + a_1t + a_0)c = c^{q^m}(a_{m-1}t^{m-1} + \dots + a_1t + a_0)$$

y como $t^h c = c^{q^h} t^h$ para $h < n$, esto se escribe

$$a_{m-1}(c^{q^{m-1}} - c^{q^m})t^{m-1} + \dots + a_1(c^q - c^{q^m})t + a_0(c - c^{q^m}) = 0$$

por lo que t será raíz de una ecuación de $\gamma[x]$ de grado inferior a m , lo que es imposible. Luego los C_j^* son todos nulos y los a_{ij} también.

Probemos que estos q^{n^2} elementos distintos constituyen un subanillo de σ , que contiene estrictamente a γ , de donde resultará que este conjunto es σ . Nos basta demostrar que este conjunto, que es estable para la adición, lo es también para la multiplicación.

Esto resulta inmediatamente del hecho de que

$$a_{ij}c^j t^j a_{i'j'}c^{i'} t^{j'} = a_{ij}a_{i'j'}c^j t^j c^{i'} t^{j'}$$

se pone bajo la forma deseada reemplazando: $t^j c^{i'}$ por $(c^{q^j})^{i'} t^j$; luego, t^j , si

$$j = qn + r,$$

por ωt^r con $\omega = (t^n)^q \in \Omega$, $r < n$; y $(c^{q^j})^{i'}$ como elemento de γ por su expresión

$$\sum_{i=0}^{n-1} \omega_i c^i.$$

El orden N de σ es pues igual a q^{n^2} , donde q es el orden del centro Ω de σ . El entero n interviene en el orden q^n del subcuerpo maximal γ . Como el orden de σ es una cantidad ligada intrínsecamente a σ , resulta que todo subcuerpo maximal de σ tiene el mismo orden q^n .

Pero dos campos de Galois del mismo orden son isomorfos. Luego $\gamma = \Omega(c)$ y $\gamma_i = \Omega(c_i)$ son isomorfos sobre Ω ; y c y c_i elementos primitivos de γ y γ_i verifican la misma ecuación característica $g(x) = 0$, $g(x) \in \Omega[x]$. Ahora bien, se ha visto (§ 4, teor. 3) que dos raíces c y c_i de una misma ecuación irreducible en $\Omega[x]$, situadas en un cuerpo no conmutativo que tiene por centro Ω están ligadas por $c_i = s c s^{-1}$ con $s \in \sigma$. Resulta inmediatamente que los grupos multiplicativos $\gamma - \{0\}$ y $\gamma_i - \{0\}$ son conjugados en el grupo multiplicativo $\sigma - \{0\}$. Pero entonces el grupo finito $\sigma - \{0\}$ resultaría cubierto por los conjugados de uno de sus subgrupos γ , lo que es imposible (cap. II, § 7, teor. 4); se tiene pues $\Omega = \sigma$.

§ 10. Clausura algebraica de un cuerpo k

Consideremos un cuerpo k y un conjunto $\mathcal{F}$ de polinomios $p_i(x)$ ($i \in I$) de coeficientes en k (en particular, $\mathcal{F}$ podrá ser el conjunto de *todos* los polinomios del anillo $k[x]$). Nos proponemos demostrar que existe una extensión algebraica de k en la cual todo polinomio $p_i(x) \in \mathcal{F}$ se descompone en factores lineales; y además, que un subcuerpo K minimal entre los que tienen la propiedad precedente está determinado a menos de un k -isomorfismo.

Supondremos que, en cada polinomio $p_i(x)$, el coeficiente de la potencia más alta de x se ha reducido a la unidad. Pongamos $k' = k(x)$, cuerpo de las funciones racionales en x con coeficientes en k , e introduzcamos un conjunto $\{y_{i,j}\}$ de indeterminadas $y_{i,j}$ dependientes de dos índices: el primer índice, i , recorre el conjunto I de índices del conjunto $\mathcal{F}$ de polinomios $p_i(x)$ considerado; fijado i , el segundo índice, j , recorre el conjunto $\{1, 2, \dots, n_i\}$ donde n_i es el grado del polinomio $p_i(x)$. Sea D el anillo de polinomios, de coeficientes en k' , con respecto a las indeterminadas $y_{i,j}$ (cada uno de estos polinomios contiene sólo un número finito de tales indeterminadas).

Consideremos en D el ideal $\mathfrak{a}$ engendrado por los polinomios

$$f_i(x) = p_i(x) - (x - y_{i,1})(x - y_{i,2}) \dots (x - y_{i,n_i})$$

El elemento unidad e del cuerpo k no pertenece al ideal $\mathfrak{a}$, pues, si e fuera una combinación lineal de r polinomios $f_i(x)$, de coeficientes racionales en x y enteros con respecto a los $y_{i,j}$, se deduciría, reemplazando en estos polinomios los $y_{i,j}$ que figuren por las raíces de los r polinomios p_i correspondientes, una igualdad de la forma $e = 0$ (estas raíces, en número finito, son consideradas

como elementos del cuerpo de descomposición del polinomio $p(x)$, producto de los r polinomios p_i en cuestión).

Puesto que se tiene $e \notin \mathfrak{a}$, el ideal $\mathfrak{a}$ es distinto de D ; está contenido en un ideal maximal $\mathfrak{m}$ ($\neq D$) (cap. VI, § 2; esta proposición se apoya en el axioma de Zorn) el anillo cociente $D/\mathfrak{m}$ es un cuerpo Λ .

Dos elementos distintos de k pertenecen a dos clases distintas módulo $\mathfrak{m}$, sin lo cual tendríamos $e \in \mathfrak{m}$ y $\mathfrak{m} = D$. Λ contiene pues un subcuerpo isomorfo a k : es una *extensión* de k .

Sea $\eta_{i,j}$ el elemento de $\Lambda = D/\mathfrak{m}$ igual a la clase módulo $\mathfrak{m}$ que contiene el elemento $y_{i,j}$ de D . Consideremos el cuerpo intermedio K ,

$$k \subseteq K \subseteq \Lambda$$

obtenido adjuntando a k el conjunto de los $\eta_{i,j}$. Puesto que tenemos, en D ,

$$f_i(x) \in \mathfrak{m}, \quad \text{es decir} \quad f_i(x) \equiv 0 \pmod{\mathfrak{m}}$$

el polinomio $p_i(x)$, considerado como elemento del anillo $K[x]$, admite en este anillo la descomposición

$$p_i(x) = (x - \eta_{i,1})(x - \eta_{i,2}) \dots (x - \eta_{i,x_i})$$

El polinomio se descompone completamente, sobre K , en factores lineales; además, cada $\eta_{i,j}$ que anula a $p_i(x) \in k[x]$, es algebraico sobre k y, por consiguiente, k es extensión algebraica de k .

K es una extensión minimal con las propiedades precedentes pues un subcuerpo propio K' de K no contiene todos los $\eta_{i,j}$ y por consiguiente uno al menos de los polinomios p_i no se descompone, sobre K' , en factores todos lineales.

Probemos, finalmente, que *este cuerpo K está definido a menos de un k -isomorfismo*, y para ello, que si K_1, K_2 son dos de tales extensiones, existe un k -isomorfismo que aplica K_1 sobre K_2 .

Sea $\mathfrak{J}$ el conjunto de los k -isomorfismos φ que aplican un cuerpo H_1 comprendido entre k y K_1 , sobre un cuerpo H_2 comprendido entre k y K_2 :

$$(\varphi) \quad H_1 \simeq H_2 = \varphi(H_1), \quad k \subseteq H_1 \subseteq K_1, \quad k \subseteq H_2 \subseteq K_2.$$

$\mathfrak{J}$ no es vacío puesto que el automorfismo idéntico de k pertenece a $\mathfrak{J}$ ($H_1 = k = H_2$). Si φ' pertenece a $\mathfrak{J}$ y aplica H'_1 sobre H'_2 , ponemos

$$\varphi \leq \varphi' \quad \text{si} \quad \begin{cases} H_1 \subseteq H'_1 \\ H_2 \subseteq H'_2 \\ \varphi \text{ es la restricción a } H_1 \text{ de } \varphi'. \end{cases}$$

La relación así definida en $\mathfrak{J}$ es una *relación de orden*. Para esta relación de orden, $\mathfrak{J}$ es *inductivo*. Sea en efecto $\mathcal{C}$ una cadena de isomorfismos φ extraída de $\mathfrak{J}$; los cuerpos H_1 correspondientes forman una cadena $\mathcal{C}_1$, los H_2 forman una cadena $\mathcal{C}_2$. El subconjunto

$$\Delta_1 = \bigcup_{H_1 \in \mathcal{C}_1} H_1$$

de K_1 es un subcuerpo de K_1 ; igualmente

$$\Delta_2 = \bigcup_{H_2 \in \mathcal{C}_2} H_2$$

es un subcuerpo de K_2 . Consideremos la aplicación Φ de Δ_1 en Δ_2 definida de la manera siguiente: un elemento x de Δ_1 pertenece al menos a un cuerpo $H_1 \in \mathcal{C}_1$ aplicado sobre un cuerpo $H_2 \in \mathcal{C}_2$ por un isomorfismo $\varphi \in \mathcal{C}$: ponemos

$$\Phi(x) = \varphi(x) \quad (\in H_2 \subseteq \Delta_2)$$

Puesto que $\mathcal{C}$, $\mathcal{C}_1$, $\mathcal{C}_2$ son cadenas, la definición de $\Phi(x)$ no depende de la elección del sistema $\{H_1, \varphi, H_2\}$ tal que $x \in H_1$; además Φ aplica Δ_1 sobre Δ_2 y es un isomorfismo que, por construcción, es el mayorante mínimo de la cadena $\mathcal{C}$.

Según el axioma de Zorn, existe en $\mathfrak{J}$ un isomorfismo maximal Ψ , que aplica un subcuerpo L_1 de K_1 sobre un subcuerpo L_2 de K_2 . *Probemos que $L_1 = K_1$.*

Si L_1 fuese subcuerpo propio de K_1 , al menos uno de los polinomios $p_i(x) \in \mathfrak{J}$, sea $p(x)$, no se descompondría en factores lineales sobre L_1 , ni por otra parte sobre L_2 puesto que los k -isomorfismos Ψ y Ψ^{-1} hacen corresponder a toda descomposición de $p(x)$ en $L_1[x]$ una descomposición de p en factores del mismo grado en $L_2[x]$ e inversamente. Sea L'_1 el cuerpo de descomposición de $p(x)$ en K_1 , considerando $p(x)$ como polinomio de $L_1[x]$: se sabe (§ 2, teor. 1) que existe un isomorfismo Ψ' prolongación de Ψ (es decir cuya restricción a L_1 es Ψ) y que aplica L'_1 sobre L'_2 . Pero entonces, por la relación de orden introducida antes, tendríamos la *desigualdad estricta*

$$\Psi < \Psi'$$

que es imposible, puesto que Ψ es maximal.

Luego $L_1 = K_1$ y asimismo $L_2 = K_2$ (pues Ψ^{-1} es maximal con Ψ). Queda por tanto establecido el teorema.

El cuerpo K obtenido así cuando se toma como conjunto $\mathfrak{J}$ el de *todos* los polinomios del anillo $k[x]$ (o lo que viene a ser lo mismo, el conjunto de todos los polinomios irreducibles de este anillo) es por definición la *clausura algebraica* del cuerpo k .

Probemos por último que *esta clausura algebraica K es un cuerpo algebraicamente cerrado*, es decir que todo polinomio del anillo $K[x]$ (y no solamente de $k[x]$) se descompone en $K[x]$ en factores lineales, o también: el anillo $K[x]$ no contiene polinomios irreducibles de grado superior a 1.

Sea $F(x)$ un polinomio irreducible del anillo $K[x]$. Supongamos F de grado superior a 1 y sea $\theta \notin K$ un cero de F en un cuerpo de ruptura P de F :

$$k \subseteq K \subseteq P;$$

θ es algebraico sobre K que es extensión algebraica de k , luego θ es algebraico sobre k y verifica una ecuación irreducible

$$f(x) = 0 \quad \text{con} \quad f(x) \in k[x] \subseteq K[x].$$

Por consiguiente, F divide a f . Como $f(x)$ se descompone en factores lineales en $K[x]$, hay contradicción en suponer que $F(x)$ sea irreducible.

§ 11. Teorema de los ceros de Hilbert

Ahora demostraremos un teorema importante debido a Hilbert, que se designa por *teorema de los ceros*.

Dados un cuerpo conmutativo k y un ideal $\mathfrak{a}$ del anillo de polinomios $k[x_1, \dots, x_n] = A$, se llama *cero* de este ideal sobre una extensión k' de k a todo punto $(\xi_1, \dots, \xi_n) \in k'^n$ en el cual todos los polinomios del ideal $\mathfrak{a}$ toman el valor 0. Siendo noetheriano el anillo A , el ideal $\mathfrak{a}$ tendrá una base finita

$$\mathfrak{a} = (f_1, \dots, f_r), \quad f_i \in A,$$

y para que el punto $(\xi_1, \dots, \xi_n)$ sea un cero de $\mathfrak{a}$, es necesario y suficiente que los r polinomios de base f_i tomen en este punto el valor 0.

Teorema. — Si un polinomio $f \in k[x_1, \dots, x_n]$ se anula para todo cero del ideal $\mathfrak{a}$ sobre una extensión algebraicamente cerrada Ω de k , existe un exponente ρ tal que

$$f^\rho \in \mathfrak{a} = (f_1, \dots, f_r), \quad \text{o} \quad f \in \mathcal{R}(\mathfrak{a}).$$

Vamos a reducir esta demostración a la de dos lemas.

Lema 1. — Todo ideal distinto del ideal unidad $A = (e)$ (donde e indica el

elemento unidad del cuerpo k), tiene por lo menos un cero en Ω .

En efecto, supongamos el lema demostrado; en el anillo $B = k[x_1, \dots, x_n, u]$ donde u designa una nueva indeterminada, el ideal

$$\mathfrak{b} = (f_1, \dots, f_r, e - uf)$$

es un ideal que no admite ningún cero en Ω . Es pues el ideal unidad $B = (e)$ y por consiguiente existen polinomios $b_1, \dots, b_r, b_{r+1} \in B$ tales que

$$e = b_1 f_1 + \dots + b_r f_r + b_{r+1} (e - uf).$$

En esta igualdad, atribuimos a la indeterminada u el valor

$$\frac{e}{f(x_1, \dots, x_n)}$$

y transformando la ecuación en entera, obtendremos, con un conveniente número entero ρ ,

$$f^\rho = a_1 f_1 + \dots + a_r f_r, \quad \text{donde} \quad a_i(x_1, \dots, x_n) \in A.$$

El lema 1 implica pues el teorema.

Es evidente que, en toda extensión algebraicamente cerrada Ω de k , el conjunto de los elementos algebraicos sobre k es una clausura algebraica K de k (todo polinomio de $k[u]$ se descompone en $\Omega[u]$ en factores lineales cuyos ceros son algebraicos sobre k y por consiguiente pertenecen a K).

En estas condiciones, para establecer el lema 1, podemos utilizar el hecho de que todo ideal $\mathfrak{a}$ distinto del ideal unidad está contenido en un ideal maximal $\mathfrak{m}$ (cap. VI, § 2) y limitarnos a demostrar este lema para un tal ideal maximal: $\mathfrak{a} \subseteq \mathfrak{m}$ implica en efecto que todo cero de $\mathfrak{m}$ es un cero de $\mathfrak{a}$.

Ahora bien, siendo $\mathfrak{m}$ maximal, el anillo cociente $A/\mathfrak{m}$ es un cuerpo. Designemos por a_i la clase módulo $\mathfrak{m}$ que contiene el polinomio x_i ; en virtud del homomorfismo de anillos

$$A \sim A/\mathfrak{m},$$

la clase que contiene un polinomio $g(x_1, \dots, x_n)$ es la clase $g(a_1, \dots, a_n)$ y tenemos

$$A/\mathfrak{m} = k[a_1, \dots, a_n].$$

El lema 1 es, por lo tanto, consecuencia del siguiente:

Lema 2. — Si un dominio de integridad $A = k[a_1, \dots, a_n]$ sobre el cuerpo k es un cuerpo, los generadores a_i son algebraicos sobre k .

Establecido este lema, los a_i pueden ser tomados como elementos de K y, para todo polinomio $f(x_1, \dots, x_n) \in \mathfrak{m}$, $f(a_1, \dots, a_n)$ es nulo (puesto que $\mathfrak{m}$ es el núcleo del homomorfismo $A \sim A/\mathfrak{m}$); $(a_1, \dots, a_n)$ es pues un cero de $\mathfrak{m}$.

Para establecer el lema 2, observemos en primer lugar que este enunciado es evidente para $n = 1$, pues, si a_1 no es algebraico sobre k , el anillo $k[a_1]$ no es un cuerpo. Razonemos ahora por recurrencia. Puesto que $A = k[a_1, \dots, a_n]$ es un cuerpo, contiene el cuerpo $k(a_1)$, luego al anillo $k(a_1)[a_2, \dots, a_n]$ que, a su vez, contiene a $k[a_1][a_2, \dots, a_n] = A$, de donde la igualdad

$$A = k(a_1)[a_2, \dots, a_n].$$

Según la hipótesis de recurrencia $a_2, \dots, a_n$, son algebraicos sobre $k(a_1)$, luego basta probar que a_1 es algebraico sobre k .

Cada uno de los elementos $a_2, \dots, a_n$, satisface a una ecuación algebraica cuyos coeficientes pertenecen al anillo $k[a_1]$ y son los valores, para $u = a_1$, de polinomios primos entre sí en su conjunto, pertenecientes al anillo $k[u]$. Sea $c_i(u)$ el polinomio correspondiente al coeficiente director $c_i(a_1)$ de la ecuación a que satisface a_i ($i = 2, \dots, n$) y $p(u)$ el mínimo común múltiplo de los polinomios $c_i(u)$: tendremos $p(a_1) \neq 0$, y si ponemos

$$\beta_i = p(a_1)a_i \quad (i = 2, \dots, n)$$

cada uno de los elementos β_i verifica una ecuación algebraica cuyo coeficiente director es el elemento unidad e y los restantes coeficientes pertenecen a $k(a_1)$; las β_i son, pues, *enteros algebraicos* sobre $k[a_1]$. Además, para todo elemento $f(a_1, \dots, a_n)$ de $A = k[a_1, \dots, a_n]$, existe un número natural ρ tal que

$$[p(a_1)]^\rho f(a_1, \dots, a_n) = g(a_1, \beta_2, \dots, \beta_n),$$

donde $g(u_1, u_2, \dots, u_n)$ designa un polinomio en $u_1, u_2, \dots, u_n$ con coeficientes de k ; luego $g(a_1, \beta_2, \dots, \beta_n)$ es un entero algebraico sobre $k[a_1]$.

En particular, todo elemento $\varphi(a_1)$ del cuerpo $k(a_1) (\subseteq A)$ verifica una igualdad de la forma

$$[p(a_1)]^\rho \varphi(a_1) = g$$

donde g , que aquí pertenece también a $k(a_1)$, es entero sobre $k[a_1]$.

Si a_1 fuese trascendente sobre k , $a_1 = u$, el elemento g , de $k(u)$, se escribiría en forma de cociente de dos polinomios $g_1(u)$, $g_2(u)$ primos entre sí, verificando a una ecuación de la forma,

$$\left(\frac{g_1}{g_2}\right)^n + a_1 \left(\frac{g_1}{g_2}\right)^{n-1} + \dots + a_n = 0, \quad \text{donde } a_i \in k[u].$$

En el anillo $k[u]$ esta ecuación implicaría: g_2/g_1 . Entonces, o bien g_2 sería una unidad de $k[u]$, es decir un elemento de k , y tendríamos $g \in k[u]$; o bien todo factor irreducible de g_2 dividiría a g_1 , pero esto es imposible, por ser g_1 y g_2 polinomios primos entre sí.

Por último, si α_1 fuese trascendente sobre k , $\alpha_1 = u$, la fracción racional $\varphi(u)$ se escribiría en la forma

$$\varphi(u) = \frac{g(u)}{[p(u)]^p}$$

donde $g(u)$ es un polinomio y $p(u)$ un polinomio fijo. Pero esto es imposible, como se ve tomando $\varphi(u) = \frac{e}{q(u)}$, donde $q(u)$ es un polinomio primo con $p(u)$ (por ejemplo: $q(u) = p(u) + e$).

§ 12. Teoría de Galois

Dados un cuerpo K y un supercuerpo L de K , conmutativos, llamamos K -automorfismo de L a todo automorfismo de L que deja fijo cada elemento de K ¹:

$$\forall a \in K, \quad \sigma a = a.$$

El siguiente teorema implica la introducción de un concepto fundamental para lo que sigue, que es el del llamado *grupo de Galois*:

Teorema 1. — *El conjunto G de los K -automorfismos de L es un grupo, al que llamamos grupo de Galois de L sobre K , y designaremos por $G_{L:K}$. Si K' es un cuerpo intermedio entre K y L , $G_{L:K'}$ es un subgrupo de $G_{L:K}$.*

Es evidente que el automorfismo idéntico ϵ de L es un K -automorfismo, y que el inverso σ^{-1} de un K -automorfismo σ lo es también; finalmente, también el producto $\tau \circ \sigma$ de dos K -automorfismos es un K -automorfismo; por lo tanto G es un grupo (para la ley de composición $\circ$).

Si se tiene $K \subseteq K' \subseteq L$, todo K' -automorfismo de L es un K -automorfismo de L ; $G_{L:K'}$ es pues un subgrupo de $G_{L:K}$.

Teorema 2. — *El conjunto F_H de los elementos f de L que quedan invariantes en un grupo $H(\subseteq G)$ de K -automorfismos de L , es un cuerpo intermedio*

$$K \subseteq F_H \subseteq L$$

¹ Esta noción no es más que un caso particular de la de K -isomorfismo o isomorfismo sobre K , entre dos supercuerpos L, L' de K , que fue considerada anteriormente.

llamado *cuerpo fijo* (o *invariante*) de H ; la inclusión $H \subseteq H'$ implica $F_H \supseteq F_{H'}$.

Sean a y b dos elementos del conjunto F_φ de los elementos que quedan invariantes en un K -automorfismo φ . Tenemos:

$$\varphi(a - b) = \varphi(a) - \varphi(b) = a - b \quad \text{luego} \quad a - b \in F_\varphi,$$

y, si b no es nulo (lo que implica $\varphi(b) \neq 0$),

$$\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)} = \frac{a}{b} \quad \text{luego} \quad \frac{a}{b} \in F_\varphi.$$

F_φ es pues un subcuerpo de L ; el conjunto de los elementos de L que quedan invariantes por un conjunto Φ de K -automorfismos es el cuerpo

$$F_\Phi = \bigcap_{\varphi \in \Phi} F_\varphi$$

(cuerpo fijo de Φ) y $\Phi \subseteq \Phi'$ implica $F_{\Phi'} \subseteq F_\Phi$. En el enunciado, Φ y Φ' son subgrupos H y H' de G .

En resumen, a todo subgrupo H de $G_{L:K} = G$ corresponde un cuerpo intermedio F_H ; a todo cuerpo intermedio K' corresponde un subgrupo $G_{L:K'}$ de G , y cada una de estas correspondencias es antiisótoma respecto a la relación de inclusión.

Es natural considerar en particular el cuerpo fijo F_G del grupo de Galois y ver si, mediante hipótesis convenientes, F_G coincide con K .

Teorema 3. — Sean $\varphi_1, \dots, \varphi_n$ n automorfismos distintos de L . Estos automorfismos son independientes, es decir que, si n elementos $\lambda_1, \dots, \lambda_n$ de L son tales que

$$(1) \quad \sum_{i=1}^n \lambda_i \varphi_i(x) = 0 \quad \forall x \in L,$$

se tiene: $\lambda_i = 0$ ($i = 1, \dots, n$).

El teorema es evidente para $n = 1$ (puesto que se tiene $\varphi_i(x) \neq 0$ para $x \neq 0$). Demostremosle por recurrencia sobre n , suponiéndolo cierto para un número de automorfismos menor que n .

Según la hipótesis de recurrencia, es imposible que sean nulos ciertos λ_i

sin que lo sean todos; supongamos pues que son todos distintos de 0. Escribamos (1) en la forma

$$(2) \quad \sum_{i=1}^{n-1} \mu_i \varphi_i(x) + \varphi_n(x) = 0, \quad \text{con } \mu_i = \lambda_i \lambda_n^{-1} \neq 0;$$

sea a un elemento no nulo de L tal que

$$\varphi_1(a) \neq \varphi_n(a);$$

reemplazando en (2) x por ax , se tiene

$$\sum_{i=1}^{n-1} \mu_i \varphi_i(a) \varphi_i(x) + \varphi_n(a) \varphi_n(x) = 0,$$

de donde, multiplicando por $[\varphi_n(a)]^{-1}$ y restando de (2),

$$\sum_{i=1}^{n-1} \mu_i [e - \varphi_i(a) (\varphi_n(a))^{-1}] \varphi_i(x) = 0.$$

Como el coeficiente de $\varphi_1(x)$ es distinto de cero, tenemos una contradicción, según la hipótesis de recurrencia; por consiguiente $\lambda_1 = \dots = \lambda_n = 0$.

En todo lo que sigue supondremos que L es una extensión finita de K . Sea $(L : K)$ su grado.

Teorema 4. — *a) Si $\sigma_1, \dots, \sigma_m$ son m K -automorfismos distintos de L y si F es el cuerpo fijo F_Φ de $\Phi = \{\sigma_1, \dots, \sigma_m\}$, se tiene:*

$$(L : F) \geq m.$$

b) Si el conjunto de automorfismos considerado $\{\sigma_1, \dots, \sigma_m\}$ es un grupo $H(\subseteq G)$, se tiene la igualdad

$$(L : F) = m.$$

a) Pongamos $(L : F) = r$ y sea $(a_1, \dots, a_r)$ una base de L considerado como espacio vectorial sobre F .

Si fuese $r < m$, las r ecuaciones lineales

$$(3) \quad \sum_{i=1}^m \sigma_i(a_k) x_i = 0 \quad (k = 1, \dots, r)$$

tendrían soluciones no todas nulas $x_i \in L$. Sea entonces

$$l = \sum_{k=1}^r \lambda_k a_k \quad (\lambda_k \in F)$$

un elemento cualquiera de L . Puesto que F es el cuerpo fijo del conjunto de los σ_i , tenemos

$$\sigma_i(\lambda_k) = \lambda_k$$

de donde

$$\lambda_k \sigma_i(a_k) = \sigma_i(\lambda_k) \sigma_i(a_k) = \sigma_i(\lambda_k a_k)$$

y, multiplicando las ecuaciones (3) por $\lambda_1, \dots, \lambda_r$ y sumándolas, obtenemos:

$$\sum_{i=1}^m \left[\sum_{k=1}^r \sigma_i(\lambda_k a_k) \right] x_i = \sum_{i=1}^m \sigma_i(l) x_i = 0, \quad \forall l \in L;$$

$\sigma_1, \dots, \sigma_m$ no serán pues linealmente independientes, lo que según el teorema 3 es imposible.

b) Supongamos ahora que se trata de un grupo $H = \{ \sigma_1, \dots, \sigma_m \}$ de K -automorfismos de L .

Si tuviésemos $r > m$, existirían $m+1$ elementos $\nu_1, \dots, \nu_{m+1}$ de L linealmente independientes sobre F . Las m ecuaciones lineales

$$(4) \quad \sum_{i=1}^{m+1} \sigma_k(\nu_i) y_i = 0 \quad (k = 1, \dots, m)$$

tendrían soluciones $y_i \in L$ no todas nulas, soluciones que, además, no pertenecen todas a F pues, uno de los elementos del grupo H , sea σ_1 , es el automorfismo idéntico ϵ , por lo que la ecuación (4) correspondiente se escribe

$$\sum_{i=1}^{m+1} \nu_i y_i = 0$$

y, por hipótesis, los ν_i son linealmente independientes sobre F .

Entre los sistemas de soluciones no todas nulas de las ecuaciones (4), consideremos una que contenga el menor número posible μ de elementos distintos

de 0; la denotaremos por $\eta_1, \dots, \eta_\mu, 0, \dots, 0$. Tenemos además $\mu > 1$, pues $\mu = 1$ implicaría en particular

$$\eta_1 \sigma_1(\nu_1) = \eta_1 \nu_1 = 0$$

lo cual no es cierto. Podemos también tomar η_μ igual al elemento unidad e de L y escribir finalmente

$$(4') \quad \sum_{i=1}^{\mu-1} \eta_i \sigma_k(\nu_i) + \sigma_k(\nu_\mu) = 0 \quad (k = 1, \dots, m).$$

Como ya hemos visto, las η_i no están todas en F ; sea por ejemplo $\eta_1 \notin F$; existe entonces al menos un automorfismo σ_k , sea σ_p , tal que

$$\sigma_p(\eta_1) \neq \eta_1.$$

Reemplazando en (4') el índice k por el índice j y aplicando el automorfismo σ_p , obtenemos

$$\sum_{i=1}^{\mu-1} \sigma_p(\eta_i) [(\sigma_p \circ \sigma_j)(\nu_i)] + (\sigma_p \circ \sigma_j)(\nu_\mu) = 0 \quad (k = 1, \dots, m).$$

Siendo H un grupo, j puede ser elegido de manera que

$$\sigma_p \circ \sigma_j = \sigma_k.$$

Con esta elección y restando la ecuación precedente de (4'), obtenemos

$$(5) \quad \sum_{i=1}^{\mu-1} [\eta_i - \sigma_p(\eta_i)] \sigma_k(\nu_i) = 0$$

donde el coeficiente de $\sigma_1(\nu_i)$ es distinto de cero, lo que contradice la definición de μ .

El teorema precedente tiene consecuencias muy importantes. Por hipótesis, L es extensión finita de K ; sea

$$(L : K) = n.$$

El cuerpo fijo $\bar{K} = F_G$ del grupo de Galois G de L sobre K es un cuerpo intermedio, por lo que

$$(L : \bar{K}) \leq n$$

luego el orden del grupo de Galois G , igual a $(L : \bar{K})$, es a lo sumo igual al grado n de L sobre K .

Por otra parte, si H es un subgrupo de G y $F = F_H$ su cuerpo fijo, *toda* automorfismo $\sigma \in G$ que deja invariante a todo elemento de F pertenece a H puesto que, según la primera parte del teorema 4, el número total de estos automorfismos no puede exceder a $(L : F)$ y que, según la segunda parte, H es precisamente de orden $(L : F)$. H es pues el grupo de Galois de L sobre F , y en particular G es el grupo de Galois de L sobre $\bar{K}$. En otros términos, *dos subgrupos distintos de G no pueden tener un mismo cuerpo intermedio como cuerpo fijo* puesto que, cuando esto fuese, cada automorfismo de uno pertenecería también al otro.

Definición. — Diremos que una extensión finita L de K es *galoisiana* si el cuerpo fijo $\bar{K}$ del grupo de Galois $G = G_{L:K}$ coincide con K .

Teorema 5 a. — *El cuerpo de descomposición L de un polinomio separable $p(x) \in K[x]$ es una extensión galoisiana de K .*

Si $p(x)$ tiene todas sus raíces en K , se tiene $L = K$, y G se reduce al automorfismo idéntico, y $\bar{K} = L = K$.

Razonemos pues por recurrencia sobre el número de raíces de $p(x)$ no situadas en K , suponiendo el teorema cierto cuando este número sea menor que n y probándolo cuando n raíces no pertenecen a K .
Sea

$$p(x) = p_1(x) \dots p_r(x)$$

la descomposición de p en factores irreducibles en el anillo $K[x]$, con, por ejemplo, grado $p_1 = \nu > 1$. Sea α_1 una raíz de $p_1(x)$, *no perteneciente a K* ; $\alpha_1 \in L$. Puesto que p tiene menos de n raíces fuera del cuerpo $K(\alpha_1)$, L , que es también cuerpo de descomposición de p sobre este cuerpo, es una extensión galoisiana de $K(\alpha_1)$.

Ahora bien, según la hipótesis de separabilidad, las ν raíces $\alpha_1, \dots, \alpha_\nu$ de $p_1(x)$, todas situadas en el cuerpo de descomposición L , *son distintas*. El automorfismo idéntico de K se prolonga por un K -isomorfismo θ_i que aplica el cuerpo de ruptura $K(\alpha_1)$ de p_1 sobre el cuerpo de ruptura $K(\alpha_i)$, en particular α_1 sobre α_i ; y θ_i , que transforma en sí mismo el polinomio $p(x) \in K[x]$, se pro-

longa a su vez por un K -automorfismo σ_i del cuerpo de descomposición L . Como hace θ_i , σ_i aplica α_1 sobre α_i .

Sea entonces u un elemento de K , es decir un elemento que queda invariable por todo K -automorfismo de L . En particular, u es invariante por todo automorfismo del grupo de Galois de L sobre $K(\alpha_1)$, y, puesto que L es extensión galoisiana de $K(\alpha_1)$, u pertenece a $K(\alpha_1)$:

$$u = c_0 + c_1\alpha_1 + \dots + c_{\nu-1}\alpha_1^{\nu-1}, \quad (c_i \in K);$$

aplicando el automorfismo σ_i , obtenemos

$$\sigma_i u = u = c_0 + c_1\alpha_i + \dots + c_{\nu-1}\alpha_i^{\nu-1}$$

y el polinomio de grado $\nu - 1$

$$c_{\nu-1}x^{\nu-1} + \dots + c_1x + c_0 - u \in L[x]$$

admite las ν raíces distintas $\alpha_1, \dots, \alpha_\nu$, lo que exige que todos sus coeficientes sean nulos, en particular

$$u = c_0 \in K.$$

Así, tenemos $\bar{K} \subseteq K$, de donde sigue la igualdad.

Para establecer un recíproco, tendremos necesidad del lema siguiente.

Lema. — *Si una extensión finita L de K es galoisiana, entonces es separable y todo elemento a de L es raíz de un polinomio irreducible de $K[x]$ que, en $L[x]$, se descompone totalmente en factores lineales.*

Sea $G = \{\sigma_1, \dots, \sigma_s\}$, donde $\sigma_1 = \epsilon$, el grupo de Galois de L sobre K . Designemos por $\alpha_1 = a, \alpha_2, \dots, \alpha_r$ los elementos *distintos* entre $\sigma_1 a = a, \dots, \sigma_s a; \alpha_i \in L$. Puesto que G es un grupo, se tiene, cualesquiera que sean $i \in \{1, \dots, r\}$ y $j \in \{1, \dots, s\}$,

$$\sigma_j(\alpha_i) = \sigma_j[\sigma_i(a)] = \sigma_{ji}(a) \in \{\alpha_1, \dots, \alpha_r\}.$$

Vemos así que cada automorfismo σ_j permuta (biyectivamente) $\alpha_1, \dots, \alpha_r$; por consiguiente, el polinomio

$$f(x) = (x - \alpha_1) \dots (x - \alpha_r) \in L[x]$$

tiene todos sus coeficientes invariantes por cada σ_j . Puesto que L es extensión galoisiana de K , cada uno de los coeficientes pertenece a K , $f(x) \in K[x]$.

Además, $f(x)$ es irreducible sobre K . Sea en efecto $g(x)$ un polinomio de $K[x]$ que tenga por ejemplo a como raíz. Tenemos

$$g(\alpha_i) = g[\sigma_i(a)] = \sigma_i[g(a)] = \sigma_i(0) = 0;$$

g es un múltiplo de f : por consiguiente f no tiene ningún divisor propio en $K[x]$, es decir, es irreducible sobre K . Es evidente entonces que a es separable, y L es una extensión separable de K .

Teorema 5 b. — Si una extensión finita L de K es galoisiana, L es cuerpo de descomposición de un polinomio $p(x) \in K[x]$.

Sea $(a_1, \dots, a_n)$ una base de L considerado como espacio vectorial sobre K . Sea $f_i(x)$ el polinomio irreducible y separable de $K[x]$ del cual a_i es raíz, formado como se ha visto en el lema. Puesto que f_i en $L[x]$, es un producto de factores lineales, el polinomio

$$p(x) = f_1(x) \cdot \dots \cdot f_n(x)$$

se descompone completamente en factores lineales en $L[x]$. Además, un cuerpo intermedio L' sobre el cual $p(x)$ se descompone en factores lineales contiene necesariamente a $a_1, \dots, a_n$ y por consiguiente coincide con L ; L es pues cuerpo de descomposición de $p(x)$.

Observación. — Si una extensión finita L de K es galoisiana, L es extensión galoisiana de todo cuerpo intermedio.

Según los teoremas 5 a y 5 b, una extensión L finita y galoisiana de K no es otra cosa que el cuerpo de descomposición de un polinomio separable $p(x)$ de $K[x]$: estas dos nociones coinciden. El grupo de Galois $G = G_{L:K}$ se llama también grupo de la ecuación

$$p(x) = 0.$$

Teorema 6 (teorema fundamental). — a) Si una extensión finita L de K es galoisiana, cada cuerpo intermedio K' es el cuerpo fijo de un subgrupo G' de G ; designando por $i(G')$ y $O(G')$ respectivamente el índice de G' en G y su orden, se tiene:

$$(L : K') = O(G'), \quad (K' : K) = i(G').$$

El número de K -isomorfismos distintos de K' en L es $(K' : K)$.

b) Para que un cuerpo intermedio K' sea una extensión galoisiana de K , es necesario y suficiente que K' se transforme en sí mismo por todo automorfismo $\sigma \in G$, o también que G' sea subgrupo distinguido de G . El grupo de Galois de K' sobre K es entonces isomorfo al grupo cociente G/G' .

a) Como L es el cuerpo de descomposición de un polinomio separable $p(x) \in K[x]$ y este polinomio pertenece al superanillo $K'[x]$, L es también una extensión galoisiana de K' . Por consiguiente, K' es el cuerpo fijo del subgrupo

G' de G definido como el conjunto de los K -automorfismos de L que dejan invariante cada elemento de K' . Como consecuencia del teorema 4, subgrupos distintos tienen cuerpo fijo distinto y se tiene:

$$(L : K') = O(G').$$

Puesto que

$$(L : K) = (OG)$$

es

$$(K' : K) = \frac{(L : K)}{(L : K')} = \frac{O(G)}{O(G')} = i(G').$$

Todo K -automorfismo de L , $\sigma \in G$, aplica K' sobre un cuerpo intermedio $\sigma(K')$; dos automorfismos σ, τ que pertenecen a una misma clase a la izquierda respecto a G' dan la misma imagen $\sigma(x) = \tau(x)$ para todo elemento x de K' . Inversamente, la igualdad $\sigma(x) = \tau(x)$ para todo $x \in K'$, implica que $\tau \circ \sigma^{-1}$ deja invariante a todo elemento de K' , luego pertenece a G' . El índice $i(G')$ es pues el número de K -isomorfismos distintos de K' en L , que provienen de los K -automorfismos de L .

Además, cada K -isomorfismo ρ que aplica K' sobre un cuerpo K'_1 comprendido entre K y L se obtiene de la manera precedente; ρ , en efecto, transforma el polinomio $p(x)$ en sí mismo y, puesto que L es el cuerpo de descomposición de $p(x)$ que pertenece a $K'_1[x]$, ρ puede prolongarse por un K -automorfismo σ de L .

Por consiguiente, el número de K -isomorfismos distintos de K' en L es

$$i(G') = K' : K.$$

b) Al cuerpo $K'_1 = \sigma K'$, imagen isomorfa de K' , está asociado un grupo G'_1 de G fácil de determinar:

$$(6) \quad G'_1 = \sigma G' \sigma^{-1}.$$

Es evidente en efecto que todo automorfismo de $\sigma G' \sigma^{-1}$ deja invariante cada elemento de K'_1 ; tenemos pues $\sigma G' \sigma^{-1} \subseteq G'_1$; pero intercambiando K' y K'_1 , σ y σ^{-1} , obtenemos análogamente $\sigma^{-1} G'_1 \sigma \subseteq G'$, de donde sigue la igualdad (6).

Sea ahora Γ' el grupo de los K -automorfismos de K' . Si K' es una extensión galoisiana de K , se tiene:

$$(7) \quad (K' : K) = O(\Gamma').$$

Pero inversamente, si designamos por K^* el cuerpo fijo de Γ' , tenemos

$$O(\Gamma') = (K' : K^*), \quad K \subseteq K^* \subseteq K',$$

de donde $(K^* : K) = 1$, $K^* = K$ y por consiguiente K' es extensión galoisiana de K . Así pues, la igualdad (7) es una condición necesaria y suficiente para que K' sea una extensión galoisiana de K .

Pero todo K -automorfismo de K' es un K -isomorfismo de K' en L , y el número de estos isomorfismos distintos es precisamente $(K' : K)$. La igualdad (7) expresa, pues, que $\sigma K' = K'$ para todo automorfismo $\sigma \in G$.

Ahora bien, esta igualdad, $\sigma K' = K'$, equivale a la de los subgrupos distinguidos correspondientes, es decir, a $\sigma G' \sigma^{-1} = G'$ que expresa que G' es subgrupo distinguido de G .

En estas condiciones, los K -automorfismos de K' corresponden biyectivamente a las clases de G respecto a G' , y esta correspondencia biyectiva entre G' y G/G' es un isomorfismo, lo que completa la demostración.

§ 13. Algunos complementos sobre las propiedades del grupo de Galois de un polinomio separable $f(x) \in K[x]$

Sea $G = G_{L:K}$ el grupo de los K -automorfismos del cuerpo de descomposición L de $f(x)$ sobre K ; se dice también que G es el grupo de Galois del polinomio f o de la ecuación $f = 0$.

Sean $\alpha_1, \dots, \alpha_n$ las n raíces (distintas) de f . Tenemos

$$L = K(\alpha_1, \dots, \alpha_n) = K[\alpha_1, \dots, \alpha_n]$$

puesto que, como hemos visto, siendo las α_i algebraicas sobre K , el anillo $K[\alpha_1, \dots, \alpha_n]$ es un cuerpo.

Siendo todo elemento de L una expresión polinómica en $\alpha_1, \dots, \alpha_n$ con coeficientes en K , un automorfismo $\sigma \in G$ está determinado si nos dan las imágenes $\sigma(\alpha_i)$ ($i = 1, \dots, n$), que son sendas α_j puesto que

$$f[\sigma(\alpha_i)] = \sigma[f(\alpha_i)] = \sigma(0) = 0.$$

Además, por ser σ una biyección de L , realiza una permutación $\bar{\sigma}$ de raíces $\alpha_1, \dots, \alpha_n$: a todo $\sigma \in G$ corresponde así una permutación del conjunto $\{\alpha_1, \dots, \alpha_n\}$ y σ está determinado por $\bar{\sigma}$.

Así, el grupo de Galois G de $f(x)$ se corresponde biyectivamente con un subconjunto G del grupo de las permutaciones de $\{\alpha_1, \dots, \alpha_n\}$ y, como al automorfismo compuesto corresponde la permutación producto, G es un grupo isomorfo con G .

Teorema 1. — *El grupo de Galois $G = G_{L:K}$ del polinomio separable $f(x)$ es isomorfo a un subgrupo G del grupo de permutaciones del conjunto $\{\alpha_1, \dots, \alpha_n\}$ de raíces de la ecuación $f(x) = 0$.*

Corolario. — *El orden del grupo de Galois del polinomio separable f de grado n , es un divisor de $n!$*

Nota. — A dos raíces α, α' de un mismo factor irreducible f_1 de f corresponde un isomorfismo de los cuerpos de ruptura $K(\alpha), K(\alpha')$, aplicando α sobre α' . Este isomorfismo se prolonga por un K -automorfismo del cuerpo de descomposición L de f , pues α y α' pertenecen a una misma clase de transitividad del grupo $\bar{G}$. Inversamente, según el lema del § 12, las raíces pertenecientes a una misma clase de transitividad son los ceros de un mismo polinomio irreducible de $K[x]$, divisor de f . Las clases de transitividad del grupo $\bar{G}$ se corresponden, pues, biyectivamente con los factores irreducibles (distintos) del polinomio f ; de aquí resulta que $\bar{G}$ es transitivo si y solamente si f es irreducible.

Caracterizamos el grupo $\bar{G}$ buscando en qué condición una permutación σ^* de las raíces $\alpha_1, \dots, \alpha_n$ del polinomio separable $f(x) \in K[x]$ es la restricción al conjunto $\{\alpha_1, \dots, \alpha_n\}$ de un K -automorfismo σ de L ($\sigma \in G_{L:K}$).

Es fácil obtener una *condición necesaria*. Sea $g(x_1, \dots, x_n)$ un polinomio con coeficientes en K , $g \in K[x_1, \dots, x_n]$, tal que

$$g(\alpha_1, \dots, \alpha_n) = 0.$$

Entonces, para todo $\sigma \in G_{L:K}$, se tiene:

$$\sigma(g(\alpha_1, \dots, \alpha_n)) = 0 = g(\sigma\alpha_1, \dots, \sigma\alpha_n) = g(\sigma^*\alpha_1, \dots, \sigma^*\alpha_n),$$

de donde obtenemos la *condición necesaria*:

(C) Para todo polinomio $g \in K[x_1, \dots, x_n]$ tal que $g(\alpha_1, \dots, \alpha_n) = 0$, se debe tener $g(\sigma^*\alpha_1, \dots, \sigma^*\alpha_n) = 0$.

Demostraremos que la *condición necesaria* (C) es también suficiente. Todo elemento l de L se escribe, al menos de una manera, bajo la forma de una suma finita.

$$(1) \quad l = \sum c_i \alpha_1^{\lambda_1} \dots \alpha_n^{\lambda_n} \quad (c_i \in K)$$

y tenemos

$$\forall \sigma \in G_{L:K}, \quad \sigma l = \sum c_i (\sigma\alpha_1)^{\lambda_1} \dots (\sigma\alpha_n)^{\lambda_n};$$

σ se determina pues por su restricción en el conjunto $\Lambda = \{\alpha_1, \dots, \alpha_n\}$. Sea entonces σ^* una permutación de Λ que satisface la condición (C); en todo elemento l de L , dado por una representación (1), asociamos

$$\sum c_i (\sigma^*\alpha_1)^{\lambda_1} \dots (\sigma^*\alpha_n)^{\lambda_n};$$

definimos así una aplicación σ de L en sí misma: en efecto si l admite otra representación

$$l = \sum c'_j \alpha_1^{\lambda'_1} \dots \alpha_n^{\lambda'_n},$$

el polinomio

$$g(x_1, \dots, x_n) = \sum c_i x_1^{\lambda_1} \dots x_n^{\lambda_n} - \sum c'_j x_1^{\lambda'_1} \dots x_n^{\lambda'_n}$$

es tal que

$$g(\alpha_1, \dots, \alpha_n) = 0;$$

tenemos pues por hipótesis

$$g(\sigma^* \alpha_1, \dots, \sigma^* \alpha_n) = 0$$

y en consecuencia la transformada de l es independiente de la representación (1) utilizada.

Por construcción, la transformada de $l+l'$ o de ll' es visiblemente la suma o el producto de las transformadas de l y l' ; la aplicación σ es pues un endomorfismo del cuerpo L ; además, σ deja fijo cada elemento de K . Es decir, que un cuerpo admite el endomorfismo cuando éste sea un automorfismo, salvo cuando la imagen se reduce a (0), puesto que el núcleo debe ser un ideal y un cuerpo no tiene ideal propio. Siendo el elemento unidad de K su propia imagen, σ es un *automorfismo de L sobre K* , prolongando la permutación σ^* dada del conjunto Λ de las raíces.

Ejemplo. — *Grupo de Galois de la ecuación binomia.*

Consideremos, sobre el cuerpo K , la *ecuación binomia*.

$$(1) \quad x^n - a = 0 \quad (a \in K, a \neq 0).$$

Supongamos que el grado n no es múltiplo de la característica (condición siempre cumplida si K es de característica nula): el polinomio $x^n - a$ es, pues, separable. Supongamos también que el cuerpo K contiene una raíz n -ésima primitiva de la unidad ζ (y como consecuencia todas las raíces n -ésimas de la unidad).

Si θ es una raíz de la ecuación (1), las otras son $\zeta \theta, \dots, \zeta^{n-1} \theta$; si ζ pertenece a K , el cuerpo de descomposición L de $x^n - a$ sobre K es

$$L = K(\theta).$$

Teorema 2. — Si, sobre el cuerpo K , una ecuación $f(x) = 0$ es resoluble por radicales, su grupo de Galois es resoluble.

Señalemos una consecuencia importante del teorema precedente: si se llama ecuación general de grado n la ecuación de grado n cuyos coeficientes son indeterminados (sobre un cuerpo primo), se puede demostrar que el grupo de Galois de la ecuación general de grado n es el grupo simétrico S_n y que, para $n \geq 5$, este grupo S_n no es resoluble. Resulta, pues, según el teorema 2, que, para $n \geq 5$, la ecuación general de grado n no es resoluble por radicales.

Finalmente, el teorema 2 admite, mediante algunas hipótesis suplementarias, un recíproco basándose en la propiedad siguiente.

Teorema 3. — Sea L una extensión galoisiana, de grado n , del cuerpo K que contiene las raíces de la unidad. Si el grupo de Galois $G_{L:K}$ es cíclico, L está engendrado por una raíz de ecuación binomia.

Siendo L cuerpo de descomposición de un polinomio separable de $K[x]$ es, según el teorema del elemento primitivo, extensión simple de $K : L = K(\theta)$. Sea σ un generador del grupo de Galois $G = G_{L:K}$, cíclico de orden $(L : K) = n$; tenemos: $\sigma^n = \varepsilon$, designando ε al automorfismo idéntico.

Los n automorfismos distintos $\varepsilon, \sigma, \dots, \sigma^{n-1}$ de L son independientes de K (§ 12, teorema 3) y, particularmente, es imposible que se tenga:

$$\forall l \in L, \quad l + \zeta \cdot \sigma l + \dots + \zeta^{n-1} \cdot \sigma^{n-1} l = 0.$$

Por consiguiente, puesto que todo elemento l de L es una expresión polinomial en θ de grado $n-1$ o mayor, con coeficientes en K , es imposible que los elementos

$$r_\lambda = \theta^\lambda + \zeta \cdot \sigma \theta^\lambda + \dots + \zeta^{n-1} \cdot \sigma^{n-1} \theta^\lambda, \quad (\lambda = 1, \dots, n-1)$$

sean todos nulos ($r_0 = e + \zeta + \dots + \zeta^{n-1} = 0$, donde e designa el elemento unidad de K). Sea pues $r \neq 0$ ($1 \leq \mu \leq n-1$). Adoptamos $r = r_\mu$.

Tenemos:

$$(2) \quad \sigma r = \sigma \theta^\mu + \zeta \cdot \sigma^2 \theta^\mu + \dots + \zeta^{n-1} \cdot \theta^\mu = \zeta^{-1} r,$$

de donde

$$\sigma(r^n) = (\sigma r)^n = \zeta^{-n} r^n = r^n.$$

Así pues, r^n es invariante por σ y como consecuencia por todo automorfismo $\tau = \sigma^\nu \in G$; es, por tanto, un elemento del cuerpo K :

$$r^n = a \in K;$$

luego, r es raíz de una ecuación binomia de grado n sobre el cuerpo K .

La ecuación (2) implica:

$$(3) \quad \sigma^{\nu} r = \zeta^{-\nu} r \neq r \quad (\nu = 1, \dots, n-1)$$

puesto que ζ es raíz n -ésima *primitiva*. El único automorfismo, en $G = (\sigma)$, que deja invariante a r es, pues, la identidad de ε : el grupo de Galois $G_{L:K(r)}$ se reduce, por tanto, necesariamente a (ε) , lo cual implica:

$$[L : K(r)] = 1, \quad \text{de donde} \quad L = K(r).$$

De este teorema resulta:

Teorema 4. — *Una ecuación $f(x) = 0$, sobre el cuerpo K considerado, cuyo grupo de Galois G sea resoluble, es resoluble por radicales.*

Basta considerar una serie de composición de G y aplicar el teorema 3 a cada grupo cociente de esta serie.

Un estudio más profundo, que no haremos aquí, del *polinomio circular* $\Phi_n(x)$, es decir, del polinomio que tiene por raíces las raíces *primitivas* n -ésimas de la unidad, permite reemplazar la hipótesis de que K es de característica nula y contiene todas las raíces de la unidad, por unas hipótesis menos restrictivas.

INDICE ALFABETICO

- Abeliano (Conjunto), 29
- (Grupo), 48
- libre (Grupo), 109
- Abelización de un grupo, 85
- Absorción (Ley), 200
- Acotado (Subconjunto), 186
- Adición de aplicaciones lineales, 327
- de matrices, 332
- Aditiva (Notación), 3
- Aditivo (Grupo), 278
- Aditivos (Grupos), 51
- Adjunción simbólica, 371
- Adjunta (Matriz), 364
- Aisladas (Partes), 46.
- Algebra, 111
- asociativa, 278, 370
- Algebraicamente cerrado (Cuerpo), 391
- Algebraicas (Ecuaciones), 383
- Algebraico (Elemento), 369
- Alzado de una equivalencia, 12
- A — módulos, 276
- Anillo, 116
- (Característica), 129
- (Centro), 336
- (Extensión simple), 123
- (Grupo aditivo), 129
- (Ideales), 162
- (Propiedades aritméticas), 148
- cociente, 118
- con elemento unidad, 117.
- con factorización única, 149
- conmutativo, 116
- de división, 124
- de las clases de restos, 118
- de las series formales, 136
- de los enteros, 123
- — de Gauss, 123
- — módulos m , 118
- de los números complejos, 123
- — racionales, 123
- euclídeo, 155
- — (Ejemplos), 155
- factorial, 149
- gaussiano, 149
- íntegro, 120
- — (Característica), 131
- Noetheriano, 263
- Anillo principal, 268
- producto, 118
- Anillos (Homomorfismo), 180
- noetherianos, 265
- Anti-isomorfismo, 209
- Antisimétrica (Relación), 183
- Anulador a la derecha, 165
- Aplicación (Equivalencia), 12
- biunívoca, 3
- biyectiva, 3, 23
- canónica, 22
- compuesta, 4
- exhaustiva, 3
- inyectiva, 3
- lineal (Matriz), 330
- — (Rango), 339
- — singular, 340
- Aplicaciones biyectivas, 41
- exhaustivas, 41
- idempotentes, 329
- iguales, 326
- inyectivas, 41
- lineales, 326
- — (Adición), 327
- Aritméticas (Congruencias), 16
- Asociados (Elementos), 148
- Asociativa (Algebra), 370
- (Ley), 39
- (Multiplicación de ideales), 173
- Asociatividad, 38
- mixta (Condición), 69
- Atomo, 185
- Automorfismo, 20
- idéntico, 20
- Automorfismos, 340
- internos, 66
- Axioma de elección
- de los cocientes, 31
- de Zermelo, 259
- de Zorn, 249, 259
- — (Aplicaciones), 252
- Axiomas equivalentes al de Zorn, 256
- Base (Cambio), 347
- (Ejemplo de investigación), 171.
- de filtro, 195
- finita (Espacios vectoriales), 320

- Base finita de un ideal, 170
- Bases de un espacio vectorial, 319
- Bezout (Identidad), 270
 - (Relación), 96
- Bilátero (Ideal), 163
- Binaria (Operación), 2
- Biunívoca (Aplicación), 3
- Biyectiva (Aplicación), 3, 23, 41
- Biyectivo (Dominio de operadores), 69
- Boole (Retículo), 209
- Buena ordenación, 256

- Cadena, 183, 288
 - ascendente (Condición), 264
 - descendente (Condición), 265
- Cambio (Teorema), 304, 324
 - de base, 347
- Campo de Galois, 392, 399
 - — (Número de elementos), 400
 - raíz, 374
- Campos de Galois, 125
- Cancelable (Elemento), 26
- Cancelativa (Regla), 26
- Canónica (Aplicación), 22
- Canónico (Homomorfismo), 22, 60
 - (Isomorfismo), 63
- Característica de un anillo, 129
 - — íntegro, 131
- Casi primario (Ideal), 237
- Cayley (Teorema), 72
- Central (Elemento), 29
- Centro de un anillo, 336
- Cero (Clase), 126
 - (Divisor), 120
 - (Elemento), 27
 - (Ideal), 164
 - aditivo, 27
 - de un ideal, 412
 - multiplicativo, 27
- Cíclico (Grupo), 94
- Ciclo de longitud, 91
- Clase cero, 126
 - unidad, 60
- Clases, 11
 - (Descomposición), 62
 - de restos, 62
 - — (Anillo), 118
 - residuales módulo m , 17
 - — — (Conjunto), 17
- Clausura algebraica, 409
 - de Moore, 168, 191
 - — (Aplicación), 9
- Cociente (Anillo), 118
 - (Conjunto), 60.
 - (Grupo), 60
 - (Semigrupo), 43
- Cocientes (Axioma), 31
 - (Cuerpo), 127
- Coeficiente director, 139
 - principal, 139
- Coeficientes de combinación lineal, 317
- Cogrupos, 62
- Combinación lineal, 317
 - — (Coeficientes), 317
- Compatible (Subgrupo), 278
- Complejos, 56
- Complementación de la base (Teorema), 324
- Complementado (Retículo), 207
- Complemento, 206
- Completo (Inf-semirretículo), 189
 - (Retículo), 189, 280
- Componentes, 298
 - aislado de la intersección, 246
- Composición (Leyes), 2
 - (Serie), 290
 - asociativa (Leyes), 41
 - conmutativa (Ley), 29
 - interna (Ley), 2, 46, 69
 - — definida totalmente, 3
 - uniforme (Ley), 3
- Compuesta (Aplicación), 4
- Condición de asociatividad mixta, 68
 - de cadena ascendente, 264
 - — descendente, 265
 - de Gauss, 150, 269
 - maximal, 262
 - minimal, 265
- Congruencias aritméticas, 16
 - — (Módulo), 16
- Conjuntista (Intersección), 86
- Conjunto (Partición), 11
 - (Permutaciones), 41, 52
 - (Transformaciones), 41
 - abeliano, 29
 - bien ordenado, 256
 - cociente, 60
 - conmutativo, 29
 - de clases residuales (Módulo m), 17
 - filtrante, 187
 - — inferiormente, 186
 - — superiormente, 186
 - finito, 5
 - inductivo, 249
 - ordenado, 183
 - — (Condición maximal), 262
 - — (Diagrama), 183
 - — (Grafo), 183
 - — fuertemente inductivo, 250.
 - producto cartesiano, 2
 - regular, 26
 - totalmente ordenado, 183, 256
- Conjuntos inductivos (Ejemplos), 249
 - isomorfos, 189
- Conmutador, 85
 - (Grupo), 85

- Conmutativa (Ley de composición), 29
 Conmutativo (Anillo), 116
 — (Conjunto), 29
 — (Cuerpo), 124
 Contribución distributiva (Leyes), 111
 Coordenadas de los vectores, 330
 Cuerpo, 124
 — (Clausura algebraica), 409
 — (Extensión), 127
 — algebraicamente cerrado, 391
 — conmutativo, 124
 — de cocientes, 127
 — de descomposición, 373
 — de fracciones, 127
 — de Galois, 392
 — de las fracciones racionales, 142
 — de ruptura, 371
 — minimal, 127
 — oblicuo, 124
 — perfecto, 391
 — primo, 128
 — raíz, 374
 Cuerpos (Ejemplos), 125

 Definición (Relaciones), 108
 Derivada, 388
 — (Propiedades), 388
 Derivado (Grupo), 85
 Descomposición (Cuerpo), 373
 — en clases, 62
 — en producto directo (Ejemplos), 296
 — noetheriana, 272
 Diagonal (Matriz), 365
 Diferencia simétrica, 212
 Dimensión de un espacio vectorial, 322
 Director (Coeficiente), 139
 — (Término), 139
 Distinguidos (Subgrupos), 57, 64, 192
 Distributiva general (Propiedad), 175
 Distributivas (Leyes generales), 204
 Distributividad, 203
 — (Multiplicación de ideales), 175
 Distributivo (Carácter de una ley), 111
 — (Retículo), 200, 203
 División (Anillo), 124
 Divisor de cero, 120
 — mínimo, 176
 — propio, 120
 — verdadero, 120
 Divisores impropios, 149
 — propios, 149
 Dominio, 111, 155
 — de integridad, 121, 180
 Dual (Relación de orden), 200
 Dualidad (Principio), 203

 Ecuación característica, 359, 360
 — de las clases, 76

 Ecuación característica,
 — matricial, 349
 — mínima de una matriz, 350
 Ecuaciones algebraicas, 383
 Ejemplos de anillos euclídeos, 155
 — de conjuntos inductivos, 249
 — de cuerpos, 125
 — de descomposición en producto directo, 296
 — de filtros, 196
 — de grupos, 51
 — de retículos no distributivos, 200
 — de subgrupos, 55
 Elección (Axioma), 259
 Elemento (complemento), 206
 — (Entero algebraico), 393
 — (Longitud), 99
 — (Polinomio característico), 369
 — (Potencia), 40
 — (Trayectoria), 70
 — algebraico, 369
 — cancelable, 26
 — central, 29
 — cero, 27
 — identidad, 27
 — inferior, 185
 — inversible, 27
 — inverso, 28
 — involutivo, 28
 — irreducible, 149
 — maximal, 185
 — máximo, 185
 — mayorante, 186
 — minimal, 186
 — mínimo, 185
 — minorante, 186
 — neutro (Unicidad), 27
 — nilpotente, 121
 — nulo, 185
 — opuesto, 28
 — primitivo (Teorema), 404
 — regular, 26
 — separable, 391
 — simplificable, 26
 — — a la derecha, 25
 — — a la izquierda, 25
 — superior, 185
 — trascendente, 369
 — unidad, 27, 117, 123
 — — (Anillo), 117
 — universal, 185
 Elementos (Producto de los tres), 39
 — asociados, 148
 — lícitos, 26
 — minorantes, 15
 — neutros, 26
 — permutables, 29
 — simétricos, 28

- Elementos simetrizables, 28
 — superfluos, 15
 Emmy Noether (Teorema), 274
 Endomorfismo, 20
 Enteros (Anillo), 123
 — algebraicos, 393
 — de Gauss (Anillos), 123
 — módulos m (Anillo), 118
 Epimorfismo, 19
 Equivalencia (Alzado), 12
 — (Relación), 17
 — (Relaciones), 12
 — (Restricción), 16
 — de aplicación, 12
 — de clausura de Moore, 14
 — del homomorfismo, 24
 — recíproca, 12
 — regular, 14
 — universal, 12
 Equivalentes (Matrices), 348
 — (Subconjuntos finitos), 303
 Escalares (Matrices), 335
 Espacio cero, 351
 — homogéneo, 76
 — — (Teorema de homomorfismo), 74.
 — imagen, 330, 339
 — — (Dimensión), 339
 — nulo, 351
 — vectorial (Bases), 319
 — — (Dimensión), 322
 — — (Subconjunto independiente), 319
 — — (Subconjunto libre), 319
 — — a la izquierda, 277
 — — monógeno, 317
 Espacios vectoriales, 276, 316
 — — de base finita, 320
 Espectro de la matriz, 360
 Estabilizador, 73
 Estable (parte —), 7; (subgrupo —), 278
 Estructura fundamental (Teorema), 311
 Euclídeo (Anillo), 155
 Exhaustivas (Aplicaciones), 3, 4
 Equivalentes (Matrices), 348
 Expresión polinómica, 134, 370
 Expresiones racionales, 135
 Extensión algebraica, 379
 — — separable, 391
 — — simple, 369
 — de dimensión finita, 379
 — de grado finito, 379
 — de un cuerpo, 127
 — finita, 379
 — — galoisiana, 420
 — infinita, 379
 — simple, 128
 — — de un anillo, 123
 — — de un cuerpo, 368
 — trascendente, 369
 Extensiva (Aplicación de clausura de Moore), 10
 Factor constante de un polinomio, 158
 — contingente, 158
 Factores de la serie normal, 288
 Factorial (Anillo), 149
 Factorización única (Anillo), 149
 Familia de los filtros, 213
 — de Moore, 8
 — — de los filtros, 193
 — de subgrupos distinguidos, 86
 — U inductiva, 250
 Familias de Moore (Intersección), 8
 Fermat (Teorema), 133
 Filtrante (Conjunto), 187
 — inferiormente (Conjunto), 186
 — superiormente (Conjunto), 186
 Filtro, 193
 — (Base), 195
 — principal, 196
 Filtros (Ejemplos), 196
 — (Familia), 213
 — (Familia de Moore), 193
 — principales (Retículo), 208
 Forma, 142
 Formales (Series), 136
 Fórmula de Leibnitz, 389
 Fracciones (Cuerpo), 127
 — racionales (Cuerpo), 142
 Función polinómica, 144
 — polinomio, 144
 — uniforme, 2
 — univalente, 3
 Funciones polinómicas, 135
 Fundamentales (Relaciones), 108
 Galvis (Campos), 125, 392, 399
 — (Cuerpo), 392
 — (Grupo), 415
 — (Teoría), 415
 Galoisiana (Extensión finita), 420
 Gauss (Anillo), 149
 — (Condición), 150, 269
 — (Teorema), 154
 Generadores (Sistema finito), 98
 — (Sistema irreducible), 15, 85, 100
 — (Sistema irreducible de dos), 89
 — (Sistema minimal), 85
 — (Sistema mínimo), 15
 — (Sistemas), 84
 Grado del polinomio, 139
 Grupo (Abelización), 85
 — (Mínimo), 100
 — (Producto directo), 291
 — (Relaciones de definición), 108
 — (Relaciones fundamentales), 108
 — (Subgrupo), 55

- Grupo abeliano, 48
 — — (Rango), 303
 — — de tipo finito, 308
 — — libre, 109
 — aditivo, 278
 — — de los enteros módulo n , 51
 — — de un anillo, 129
 — cíclico, 94
 — cociente, 60
 — conmutador, 85
 — con operadores, 80, 275
 — de Galois, 415
 — de las unidades, 123
 — derivado, 85
 — de tipo finito, 98
 — finito (Orden), 48
 — indescomponible en producto directo, 295
 — libre, 104
 — lineal, 340
 — monógeno, 93
 — — infinito, 93, 106
 — ordenado, 230
 — periódico, 95
 — primer derivado, 85
 — reticulado, 231
 — simétrico, 52, 87
 — transitivo, 75
 Grupos (Ejemplos), 51
 — aditivos, 51
 — asociados a otro dado, 53
 — — a varios subgrupos, 53
 — libres, 103
 — multiplicativos, 51
 — sin torsión, 95
 Hamilton-Cayley (Teorema), 362
 Hausdorff, 249
 Hilbert (Teorema de los ceros), 412
 Hipercomplejo (Sistema), 278
 Homogéneo (Polinomio), 142
 Homomorfa (Imagen), 19, 43
 Homomorfismo, 18
 — (Aplicación inyectiva), 19
 — (Equivalencia), 22, 24
 — (Núcleo), 59
 — (Teorema), 23
 — canónico, 22, 60
 — de anillos, 180
 — en teoría de grupos, 57
 — natural, 22
 Ideal (Base finita), 170
 — (Principal a la derecha), 170
 — (Principal a la izquierda), 170
 — a la derecha, 164
 — bilátero, 163
 — casi primario, 237
 Ideal cero, 164
 — maximal, 176, 267
 — máximo, 176
 — primario, 238
 — — fuerte, 239
 — primo, 178
 — propio, 165
 — sin divisores, 176
 — unidad, 164
 Ideales de un anillo, 162
 — maximales, 273
 — semiprimos, 234
 Idempotente (Aplicación de clausura de Moore), 10
 — (Conjunto), 26
 — (Ley de composición), 26
 Identidad (Elemento), 27
 — de Bezout, 270
 Igualdad de matrices, 332
 Imagen, 3
 — homomorfa, 19, 43, 73
 — recíproca, 3
 Impropio (Subanillo), 121
 Impropios (Divisores), 149
 Independiente (Subconjunto de un espacio vectorial), 319
 Indeterminada, 137
 Indicador (de Euler), 96
 Inducción (Principio), 6
 Inductivo (Conjunto), 249
 — (Subconjunto), 305
 Inferior (Elemento), 185
 Infimo, 188
 Inf. semirretículo, 188
 — completo, 188, 189
 Inicial (Sección), 197
 Inseparable (Polinomio), 391
 Integridad (Dominio), 121, 180
 Íntegro (Anillo), 120
 Intersección (Componente aislado), 246
 — conjuntista, 86.
 — de familias de Moore, 8
 Intersecciones normadas, 244
 Invariantes (Sistema completo), 315
 — (Subgrupos), 57, 67
 Inversible (Elemento), 27
 Inverso (Elemento), 28
 — (Isomorfismo), 20
 Involutivo (Elemento), 28
 Inyectiva (Aplicación), 3
 Inyectivas (Aplicaciones), 41
 Irreducible (Elemento), 149
 — (Polinomio), 392
 Isomorfias (Series normales), 289
 Isomorfismo, 19
 — (Primer teorema), 25
 — (Teorema segundo), 285
 — anti, 209.

- Isomorfismo canónico, 63
 - inverso, 20
 - para grupos (Primer teorema), 65
 - recíproco, 20
- Isomorfos (Conjuntos), 189
- Isótona (Aplicación de clausura de Moore), 10
 - (Multiplicación), 230
 - (Multiplicación de ideales), 174
- Isotonía de la residuación, 241
- Jordan-Hölder (Serie), 290
 - — (Teorema), 290
- Kronecker (Símbolos), 335
- k -cadena, 259
- Lasker, 274
- Leibnitz (Fórmula), 389
- Letras, 103
- Ley asociativa, 39
 - de absorción, 200
 - de composición conmutativa, 29
 - — externa a la derecha, 4, 67, 80
 - — a la izquierda, 4
 - — idempotente, 26
 - — interna, 2, 46, 69
 - — (Conjuntos), 4
 - — definida totalmente, 3
 - — uniforme, 3
- Leyes de composición, 2
 - — asociativa, 41
 - — distributiva, 111
 - distributivas generales, 204
 - multiformes, 3
- Libre (Grupo), 104
 - (Sistema), 303
 - (Subconjunto de un espacio vectorial), 319
- Libres (Grupos), 103
- Lícita (Parte), 33
- Lícito (Subconjunto), 33
 - (Subgrupo), 278
- Lícitos (Elementos), 26
- Lineales (Aplicaciones), 326
- Linealmente dependiente (Sistema), 303
 - — (Sistema de elementos), 318
 - independiente (Sistema), 303
 - — (Sistema de elementos), 318
- Longitud (Ciclo), 91
 - de la serie, 288
 - de un elemento, 99
- Mac Neille (Teorema), 196, 198
- Matriz (Espectro), 360
 - (Transposición), 341
 - (Traza), 361
 - adjunta, 364
- Matriz cero, 349
 - cuadrada, 334
 - de aplicación lineal, 331
 - de una aplicación lineal, 330
 - diagonal, 365
 - nula, 333
 - $p \times n$, 331
 - singular, 340
- Matrices (Adición), 332
 - (Columnas), 331
 - (Cuadro rectangular), 331
 - (Ecuación mínima), 350
 - (Igualdad), 332
 - (Multiplicación), 333
 - (Polinomio mínimo), 350
 - (Transformación), 348
 - (Vectores columnas), 334
 - (Vectores filas), 334
 - cuadradas, 335, 346
 - — (Centro del anillo), 336
 - equivalentes, 348
 - escalares, 335
- Maximal (Condición), 262
 - (Ideal), 176, 267
 - elemento, 185
- Maximales (Ideales), 273
- Máximo (Elemento), 185
 - (Ideal), 176
 - común divisor, 152
- Mayorado (Subconjunto), 186
- Mayorante (Elemento), 186
- Minimal (Condición), 265
 - (Cuerpo), 127
 - (Elemento), 186
- Mínimo (Elemento), 185
 - común múltiplo, 153
 - grupo, 100
 - subanillo, 122
- Minorado (Subconjunto), 186
- Minorante elemento, 186
- Minorantes (Elementos), 15
- Modular (Retículo), 218
- Módulo de tipo finito, 395
 - de una congruencia aritmética, 16
- Módulos sobre un anillo A , 276
- Monógeno (Espacio vectorial), 317
 - (Grupo), 93
 - (Subespacio vectorial), 317
 - (Subgrupo), 93
 - infinito (Grupo), 106
- Monoide, 39
- Monomio, 138, 141
- Moore (Aplicación de clausura), 9
 - (Clausura), 168, 191
 - (Equivalencia de clausura), 14
 - (Familia), 8
- Multiformes (Leyes), 3
- Multiplicación compatible de matrices, 333

- Multiplicación compatible con isótona, 230.
 Multiplicadores a la derecha, 4
 — a la izquierda, 4
 Multiplicativa (Notación), 3
 Multiplicativo (Cero), 27
 — (Notación), 39
 — (Retículo), 231
 Multiplicativos (Grupos), 51
 Múltiplos, 170
- Natural (Homomorfismo), 22
 Neutros (Elementos), 26
 Nilpotente (Elemento), 121
 No distributivos (Retículos), 200
 Noether, 263
 Noetheriana (Descomposición), 272
 Noetheriano (Anillo), 263
 Normadas (Intersecciones), 244
 Normal (Serie), 288
 — (Sucesión), 227
 Normales (Subgrupos), 57
 Notación aditiva, 3
 — multiplicativa, 3, 39
 — del homomorfismo, 59
 Núcleos (Propiedades), 352
 Nulo (Elemento), 185
 Números complejos (Anillo), 123
 — enteros (Anillo), 123
 — reales (Anillo), 123
- Oblicuo (Cuerpo), 124
 Operación algebraica (Símbolo), 3
 — binaria, 2
 Operaciones clásicas (Observaciones generales), 1
 — usuales (Símbolos propios), 3
 Operador unidad, 68
 Operadores, 275
 — (Grupo), 275
 — a la derecha, 4
 — a la izquierda, 4
 Opuesta (Relación de orden), 200
 Opuesto (Elemento), 28
 Orden (Relación), 183
 — de multiplicidad de una raíz, 387
 — de un grupo finito, 48
 — estricto (Relación), 183
 — total, 257
 Ordenado (Conjunto), 183
 — (Grupo), 230
 — (Semigrupo), 230
 Ordenados (Pares), 2
 Original, 3
- Palabra, 103
 — reducida, 103
 — vacía, 103
- Palabras reducidas iguales, 103
 Pares ordenados, 2
 Parte (Radical), 46
 — lícita, 33
 — unitaria, 35
 Partes (Semigrupo), 42
 — aisladas, 46
 — cerradas, 10
 — permutables, 30
 — semiprimas, 46
 Partición de un conjunto, 11
 Peano (Sistema), 5, 6
 Perfecto (Cuerpo), 391
 Periódico (Grupo), 95
 Permutabilidad, 141
 Permutables (Elementos), 29
 — (Partes), 30
 Permutación (Signatura), 89
 Permutaciones de un conjunto, 41, 52
 Polinómica (Expresión), 135
 — (Función), 144
 Polinómicas (Funciones), 135
 Polinomio, 139, 141
 — (Cuerpo de ruptura), 371
 — (Espacio cero), 351
 — (Espacio nulo), 351
 — (Factor constante), 158
 — (Factor contingente), 158
 — (Grado), 139
 — (Valor), 143
 — característico, 360
 — — del elemento, 369
 — homogéneo, 142
 — inseparable, 391
 — irreducible, 392
 — mínimo (Aplicación), 356
 — — de una matriz, 350
 — primitivo, 158.
 — separable, 391
 Potencia de un elemento, 40
 Primario (Ideal), 238
 — fuerte (Ideal), 239
 Primitivo (Polinomio), 158
 Primo (Cuerpo), 128
 — (Ideal), 178
 — (Subcuerpo), 128
 Principal (Anillo), 268
 — (Coeficiente), 139
 — (Filtro), 196
 — (Sucesión), 227
 — (Término), 139
 — ideal a la derecha, 170
 — — a la izquierda, 170
 Principio de dualidad, 203
 — de inducción, 6
 — de recurrencia, 6
 Producto (Anillo), 118

Producto (Conjunto), 2
 — de los tres elementos, 39
 — directo de grupos, 291
 Propia (Relación), 183
 Propiedad distributiva general, 175
 Propio (Divisa), 120
 — (Ideal), 165
 — (Subanillo), 121
 — (Subgrupo), 54
 Propios (Divisores), 149
 Proyección, 298
 Proyecciones (Teorema), 22
 Punto, 185

 Racionales (Expresiones), 135
 Radical de una parte, 46
 — de un ideal, 234
 Raíz (Orden de multiplicidad), 387
 — doble, 387
 — múltiple, 387
 — primitiva, 399
 — simple, 387
 Raíces de la unidad, 398
 Rango, 107, 313
 — de una aplicación lineal, 339
 — de un grupo abeliano, 303
 Recíproca (Equivalencia), 12
 — (Imagen), 3
 Recíproco (Isomorfismo), 20
 Recta, 361
 Recubrimiento, 11
 Recurrencia (Principio), 6
 Reducida (Palabra), 103
 Reflexiva (Relación), 12, 183
 Regla cancelativa, 26
 — de los signos, 21.
 — de simplificación, 26
 Regular (Conjunto), 26
 — (Elemento), 26
 — (Equivalencia), 14
 Relación antisimétrica, 183
 — de Bezout, 96
 — de equivalencia, 17, 78
 — de orden, 183
 — — dual, 200
 — — estricto, 183
 — — opuesta, 200
 — propia, 183
 — transitiva, 78, 183
 Relaciones de definición (Sistema irreducible), 108
 — — de un grupo, 108
 — de equivalencia, 12
 — — (Ejemplos), 12
 — fundamentales de un grupo, 108
 Representación, 3, 72
 Residuación, 240
 — (Isotonía), 241

Residuado (Retículo), 240
 Residual, 240
 Restos (Clases), 62
 Restricción de una equivalencia, 16
 — de una ley de composición, 7
 Reticulado (Grupo), 231
 Retículo, 188
 — complementado, 207
 — completo, 189, 280
 — de Boole, 209
 — de los filtros principales, 208
 — de los subespacios, 280
 — distributivo, 200, 203
 — modular, 218
 — multiplicativo, 231
 — residuado, 240
 Retículos no distributivos, 200
 — — (Ejemplos), 200
 Ruptura (Cuerpo), 371

 Schreier (Teorema), 289
 Sección inicial, 197
 Semigrupo, 39, 53
 — cociente, 43
 — de las partes, 42
 — ordenado, 230
 Semiprimas (Partes), 46
 Semiprimos (Ideales), 234
 Semirretículo (Definición algebraica), 198
 Semirretículos, 187
 Separable (Elemento), 391
 — (Extensión algebraica), 391
 — (Polinomio), 391.
 Serie (Longitud), 288
 — de composición, 290
 — de Jordan-Hölder, 290
 — normal, 288
 — — (Factores), 288
 Series formales, 136
 — — (Anillo), 136
 — normales isomorfas, 289
 Signatura, 89
 — de una permutación, 89
 Signos (Regla), 21

Signos principales:

N, Q, Q^+, Z, R, C , 1
 ϵ , 2
 X , 2
 $T, L, *, +$, 2
 $\rightarrow$, 2
 $\cap, U, \wedge$, 3
 $\mathfrak{I}(E)$, 7
 $\emptyset$, 7
 C , 7
 $\bar{U}, \bar{\cap}$, 8
 $\bar{A}$, 9
 $\bar{T}$, 9

- Σ , 11
 $E/\mathcal{R}$, 12
 $\equiv$, 12
 $\mathcal{C}_m$, 17
 $\mathbb{Z}/(m)$, 17
 $\forall, \exists$, 18
 $\sim, \simeq$, 18
 $\mathbb{R}^+, \mathcal{C}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, 51
 Δ , 57
 $\mathcal{R}_a$, 62
 $\mathcal{R}_a, \rho_a$, 75
 (E, Ω) , 76
 $A[S]$, 122
 $H(S)$, 128
 $A[x]$, 139
 A/m , 164
 (o) , 164
 (e) , 164
 $\leq, \geq, <, >, \leq, \parallel$, 183
 $\sup(a, b)$, $a \vee b$, 187
 $\inf(a, b)$, $a \wedge b$, 188 x , 197
 $\mathcal{R}(m)$, 234
 Δ -grupo, 275
 $A \times B$, $A \oplus B$, 291
 $\|a\|$, 330
 $|A|$, $\det A$, 344
 $(k': k)$, 370
 $CG(p')$, $GF(p')$, 401
 Símbolos de Kronecker, 335
 Simétrica (Diferencia), 212
 — (Relación), 12,
 — (Suma), 211
 Simétricos (Elementos), 28
 Simétrico (Grupo), 52, 87
 Simetrizable (Elemento), 28
 Simple (Extensión), 128
 Simplificación (Regla), 26
 Singular (Aplicación lineal), 340
 — (Matriz), 340
 Sistema completo de invariantes, 315
 — de elementos linealmente dependientes,
 303, 318
 — — — independientes, 318
 — de generadores, 15
 — de Peano, 5, 6
 — finito de generadores, 98
 — hipercomplejo, 278
 — irreducible de dos generadores, 89
 — — de generadores, 15, 85, 100
 — — de relaciones de definición, 108
 — libre, 303
 — ligado, 303
 — linealmente independiente, 303
 — minimal de generadores, 85
 — mínimo de generadores, 15
 Sistemas de generadores, 84
 Steinitz (Teorema), 304, 324
 Subanillo, 121
 — (Mínimo), 122
 — impropio, 121
 — propio, 121
 Subconjunto acotado, 186
 — independiente de un espacio vectorial,
 319
 — inductivo, 305
 — libre de un espacio vectorial, 319
 — lícito, 33
 — mayorado, 186
 — minorado, 186
 — unitario, 35
 Subconjuntos finitos equivalentes, 303
 Subcuerpo, 127
 — primo, 128
 Subespacio, 279
 — suplementario, 320
 — vectorial monógeno, 317
 Subespacios, 316
 Subgrupo, 53
 — compatible, 278
 — estable, 278
 — lícito, 278
 — monógeno, 93
 — propio, 54
 — verdadero, 54
 Subgrupos (Ejemplos), 55
 — (Unión completa), 86
 — conjugados, 79
 — de Sylow, 81
 — de un grupo, 55
 — distinguidos, 57, 64, 192
 — — (Familia), 86
 — invariantes, 57, 67
 — normales, 57
 Subideal, 167
 Submódulos, 279
 Subretículo, 189
 Subsemigrupo, 42
 Sucesiones, 117
 Sucesión normal, 227
 — principal, 227
 Suma simétrica, 211
 Superanillo, 122
 Supercuerpo, 127
 Superideal, 167
 Superior (Elemento), 185
 Superfluos (Elementos), 15
 Suplementario (Subespacio), 320
 Supremo, 187
 Sup-semirretículo, 187
 — completo, 187
 Sustituciones, 41, 52
 Sylow (Primer teorema), 79.
 — (Segundo teorema), 80

- Teorema de Cauchy**, 81
 — de Cayley, 72
 — de Emmy Noether, 274
 — de estructura fundamental, 311
 — de Fermat, 133
 — de Gauss, 154
 — de Hamilton-Cayley, 362
 — de Jordan-Hölder, 290
 — de la complementación de la base, 324
 — de la existencia de suplementario, 324
 — de las proyecciones, 22
 — del cambio, 304, 324
 — del elemento primitivo, 404
 — del homomorfismo, 23
 — de los ceros de Hilbert, 412
 — de Mac Neille, 196, 198
 — de Schreier, 289
 — de Steinitz, 304, 324
 — de transferencia, 157
 — de von Dyck, 109
 — de Wedderburn, 125, 406
 — de Zassenhaus, 288
 — de Zermelo, 261
 — primero del isomorfismo, 25
 — — — para grupos, 65
 — segundo de isomorfismo, 285
Teoremas de Sylow, 67
 — de transferencia, 139
Teoría de Galois, 415
 — de grupos (Homomorfismo), 57
Término director, 139
 — principal, 139
Torsión (Grupo), 95
Total (Orden), 257
Transferencia (Teoremas), 139, 157
Transformación de matrices, 348
Transformaciones de un conjunto, 41
Transformado de un elemento por otro, 58
Transitiva (Relación), 12, 78, 183
Transposición de una matriz, 341
Trascendente (Extensión), 369
Trasposición, 87
Trayectoria de un elemento, 69
Traza de la matriz, 361
Ultrafiltro, 217
Unicidad del elemento neutro, 27
Unidad (Clase), 60
 — (Elemento), 27, 117, 133
 — (Ideal), 164
 — (Raíces), 398
Unidades (Grupo), 123
Uniforme (Función), 2
Unión, 187
 — completa de subgrupos, 86
Unitaria (Parte), 35
Unitario (A-módulo), 276
 — (Subconjunto), 35
Univalente (Función), 3
Universal (Elemento), 185
 — (Equivalencia), 12
Vacía (Palabra), 103
Valor del polinomio, 143
Valores característicos, 360
 — propios, 360
Vector propio, 361
Vectores, 316
 — (Coordenadas), 330
 — columnas (Matrices), 334
 — de n coordenadas, 277
Verdadero (Divisor), 120
 — (Subgrupo), 54
Von Dyck (Teorema), 109
Wedderburn (Teorema), 125, 406
Zariski-Samuel, 274
Zassenhaus (Teorema), 288
Zermelo, 249
 — (Axioma), 258
 — (Teorema), 261
Zorn, 249
 — (Axioma), 249
 — (Axiomas equivalentes), 256

